



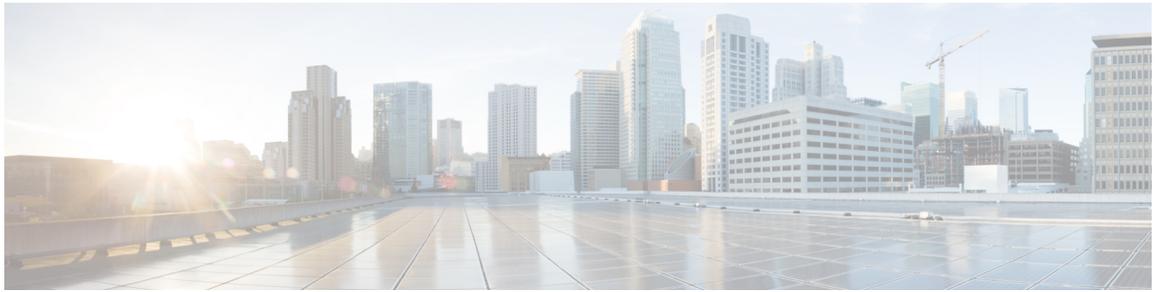
Cisco IOS XE Amsterdam 17.3.x (Catalyst 9200 スイッチ) コマンド リファレンス

First Published: 2020-07-31

Last Modified: 2020-11-07

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

コマンドライン インターフェイスの使用	1
コマンドライン インターフェイスの使用	2
コマンドモードについて	2
ヘルプシステムについて	4
コマンドの省略形	4
コマンドの no 形式および default 形式の概要	5
CLI のエラーメッセージについて	5
コンフィギュレーション ロギング の使用方法	6
コマンド履歴の使用	6
コマンド履歴バッファ サイズの変更	6
コマンドの呼び出し	7
コマンド履歴機能の無効化	7
編集機能の使用	7
編集機能の有効化および無効化	7
キーストロークによるコマンドの編集	8
画面幅よりも長いコマンドラインの編集	10
show および more コマンド出力の検索およびフィルタリング	11
CLI のアクセス	11
コンソール接続または Telnet による CLI アクセス	12

PART I

Cisco SD-Access 13

CHAPTER 2

Cisco SD-Access コマンド 15

broadcast-underlay	17
database-mapping	18
dynamic-eid	20
eid-record-provider	21
eid-record-subscriber	22
eid-table	23
encapsulation	25
etr	26
etr map-server	27
extranet	29
first-packet-petr	30
instance-id	32
ip pim lisp core-group-range	33
ip pim lisp transport multicast	34
ip pim rp-address	35
ip pim sparse mode	36
ipv4 multicast multitopology	37
ip pim ssm	38
itr	39
itr map-resolver	40
locator default-set	41
locator-set	42
map-cache	43
map-cache extranet	44
prefix-list	45
route-import database	46
service	48
show lisp instance-id ipv4 database	49
show lisp instance-id ipv6 database	51
show lisp instance-id ipv4 map-cache	52
show lisp instance-id ipv6 map-cache	58
show lisp instance-id ipv4 server	60
show lisp instance-id ipv6 server	62
show lisp instance-id ipv4 statistics	63

show lisp instance-id ipv6 statistics	64
show lisp prefix-list	65
show lisp session	66
use-petr	67

PART II**Cisco TrustSec 69**

CHAPTER 3**Cisco TrustSec コマンド 71**

address (CTS)	73
clear cts environment-data	75
clear cts policy-server statistics	76
content-type json	77
cts authorization list	78
cts change-password	80
cts credentials	81
cts environment-data enable	83
cts policy-server device-id	84
cts policy-server name	85
cts policy-server order random	86
cts policy-server username	87
cts refresh	89
cts rekey	91
cts role-based enforcement	92
cts role-based l2-vrf	94
cts role-based monitor	96
cts role-based permissions	98
cts role-based sgt-caching	100
cts role-based sgt-map	101
cts sxp connection peer	104
cts sxp default password	107
cts sxp default source-ip	109
cts sxp filter-enable	111
cts sxp filter-group	112
cts sxp filter-list	114

cts sxp log binding-changes	116
cts sxp reconciliation period	117
cts sxp retry period	118
debug cts environment-data	119
debug cts policy-server	121
port (CTS)	122
propagate sgt (cts manual)	123
retransmit (CTS)	125
sap mode-list (cts manual)	126
show cts credentials	128
show cts environment-data	129
show cts interface	130
show cts policy-server	133
show cts role-based counters	136
show cts role-based permissions	138
show cts server-list	140
show cts sxp	143
show platform hardware fed switch active fwd-asic resource team utilization	146
show platform hardware fed switch active sgacl resource usage	148
show platform software classification switch active F0 class-group-manager class-group client acl all	149
show platform software cts forwarding-manager switch active F0 port	150
show platform software cts forwarding-manager switch active F0	154
show platform software cts forwarding-manager switch active F0 permissions	155
show platform software fed switch active acl counters hardware inc SGACL	157
show platform software fed switch active acl usage	158
show platform software fed switch active ifm mappings	159
show platform software fed switch active ip route	162
show platform software fed switch active sgacl detail	164
show platform software fed switch active sgacl port	165
show platform software fed switch active sgacl vlan	167
show platform software status control-processor brief	168
show monitor capture <name> buffer	169
timeout (CTS)	170

tls server-trustpoint 171

PART III

インターフェイスおよびハードウェア コンポーネント 173

CHAPTER 4

インターフェイスおよびハードウェア コマンド 175

bluetooth pin 178

clear coap database 179

clear macro auto configuration 180

coap endpoint (COAP プロキシ コンフィギュレーション) 181

debug coap 182

device classifier 183

debug ilpower 184

debug interface 185

debug lldp packets 187

debug platform poe 188

debug platform software fed switch active punt packet-capture start 189

duplex 191

errdisable detect cause 193

errdisable recovery cause 196

errdisable recovery cause 199

interface 202

interface range 205

ip mtu 207

ipv6 mtu 209

list (COAP プロキシ コンフィギュレーション) 211

lldp (インターフェイス コンフィギュレーション) 212

logging event power-inline-status 214

macro 215

macro auto 218

macro auto apply (Cisco IOS シェルのスクリプト機能) 221

macro auto config (Cisco IOS シェルのスクリプト機能) 223

macro auto control 224

macro auto execute 226

macro auto global control	233
macro auto global processing	235
macro auto mac-address-group	236
macro auto processing	238
macro auto sticky	239
macro auto trigger	240
macro description	242
macro global	243
macro global description	246
max-endpoints (COAP プロキシ コンフィギュレーション)	247
mdix auto	248
monitoring	249
network-policy	251
network-policy profile (グローバル コンフィギュレーション)	252
port-dtls (COAP プロキシ コンフィギュレーション)	253
port-unsecure (COAP プロキシ コンフィギュレーション)	254
power-priority	255
power inline	257
power inline police	261
power supply	264
power supply autoLC shutdown	266
resource directory (COAP プロキシ コンフィギュレーション)	267
security (COAP プロキシ コンフィギュレーション)	268
shell trigger	269
show beacon all	271
show coap dtls endpoints	272
show coap endpoints	273
show coap globals	274
show coap resources	275
show coap stats	276
show coap version	277
show device classifier attached	278
show device classifier clients	280

show device classifier profile type	281
show environment	284
show errdisable detect	287
show errdisable recovery	289
show ip interface	290
show interfaces	296
show interfaces counters	303
show interfaces switchport	306
show interfaces transceiver	309
show macro auto	313
show memory platform	316
show module	319
show network-policy profile	320
show parser macro	321
show platform hardware bluetooth	324
show platform hardware fed switch forward interface	325
show platform hardware fed switch fwd-asic counters tla	328
show platform hardware fed active fwd-asic resource tcam utilization	332
show platform resources	334
show platform software audit	335
show platform software fed switch punt cpuq rates	339
show platform software fed switch punt packet-capture display	341
show platform software fed switch punt rates interfaces	343
show platform software ilpower	346
show platform software memory	348
show platform software process list	355
show platform software process memory	359
show platform software process slot switch	362
show platform software status control-processor	364
show platform software thread list	367
show processes cpu platform	369
show processes cpu platform history	372
show processes cpu platform monitor	375
show processes memory	377

show processes memory platform	381
show processes platform	385
show shell	388
show system mtu	391
show tech-support	392
show tech-support bgp	394
show tech-support diagnostic	398
speed	400
start (COAP プロキシ コンフィギュレーション)	402
stop (COAP プロキシ コンフィギュレーション)	403
switchport block	404
system mtu	406
transport (COAP プロキシ コンフィギュレーション)	407
voice-signaling vlan (ネットワークポリシー コンフィギュレーション)	408
voice vlan (ネットワークポリシー コンフィギュレーション)	410

PART IV
IP アドレッシングサービス 413

CHAPTER 5
IP アドレッシング サービス コマンド 415

clear ipv6 access-list	419
clear ipv6 dhcp	420
clear ipv6 dhcp binding	421
clear ipv6 dhcp client	423
clear ipv6 dhcp conflict	424
clear ipv6 dhcp relay binding	425
clear ipv6 eigrp	426
clear ipv6 mfib counters	427
clear ipv6 mld counters	428
clear ipv6 mld traffic	429
clear ipv6 mtu	430
clear ipv6 multicast aaa authorization	431
clear ipv6 nd destination	432
clear ipv6 nd on-link prefix	433

clear ipv6 nd router	434
clear ipv6 neighbors	435
clear ipv6 ospf	437
clear ipv6 ospf counters	438
clear ipv6 ospf events	440
clear ipv6 pim reset	441
clear ipv6 pim topology	442
clear ipv6 pim traffic	443
clear ipv6 prefix-list	444
clear ipv6 rip	446
clear ipv6 route	448
clear ipv6 spd	449
fhrp delay	450
fhrp version vrrp v3	451
ip address dhcp	452
ip address pool (DHCP)	456
ip address	457
ip unnumbered	460
ip wccp	462
ipv6 access-list	468
ipv6 address-validate	472
ipv6 cef	473
ipv6 cef accounting	475
ipv6 cef distributed	478
ipv6 cef load-sharing algorithm	480
ipv6 cef optimize neighbor resolution	482
ipv6 destination-guard policy	483
ipv6 dhcp-relay bulk-lease	484
ipv6 dhcp-relay option vpn	485
ipv6 dhcp-relay source-interface	486
ipv6 dhcp binding track ppp	487
ipv6 dhcp database	489
ipv6 dhcp iana-route-add	491
ipv6 dhcp iapd-route-add	492

ipv6 dhcp-ldra	493
ipv6 dhcp ping packets	494
ipv6 dhcp pool	495
ipv6 dhcp server vrf enable	498
ipv6 flow monitor	499
ipv6 general-prefix	500
ipv6 local policy route-map	502
ipv6 local pool	504
ipv6 mld snooping (グローバル)	506
ipv6 mld ssm-map enable	507
ipv6 mld state-limit	508
ipv6 multicast-routing	510
ipv6 multicast group-range	511
ipv6 multicast pim-passive-enable	513
ipv6 nd cache expire	514
ipv6 nd cache interface-limit (global)	516
ipv6 nd host mode strict	517
ipv6 nd na glean	518
ipv6 nd ns-interval	519
ipv6 nd nud retry	520
ipv6 nd reachable-time	522
ipv6 nd resolution data limit	523
ipv6 nd route-owner	524
ipv6 neighbor	525
ipv6 ospf name-lookup	527
ipv6 pim	528
ipv6 pim accept-register	529
ipv6 pim allow-rp	530
ipv6 pim neighbor-filter list	531
ipv6 pim rp-address	532
ipv6 pim rp embedded	535
ipv6 pim spt-threshold infinity	536
ipv6 prefix-list	537
ipv6 source-guard attach-policy	540

ipv6 source-route	541
ipv6 spd mode	543
ipv6 spd queue max-threshold	545
ipv6 traffic interface-statistics	546
ipv6 unicast-routing	547
key chain	548
key-string (認証)	549
key	550
show ip ports all	552
show ipv6 access-list	554
show ipv6 destination-guard policy	557
show ipv6 dhcp	558
show ipv6 dhcp binding	559
show ipv6 dhcp conflict	562
show ipv6 dhcp database	563
show ipv6 dhcp guard policy	565
show ipv6 dhcp interface	567
show ipv6 dhcp relay binding	570
show ipv6 eigrp events	572
show ipv6 eigrp interfaces	574
show ipv6 eigrp topology	577
show ipv6 eigrp traffic	579
show ipv6 general-prefix	581
show ipv6 interface	583
show ipv6 mfib	592
show ipv6 mld groups	598
show ipv6 mld interface	601
show ipv6 mld snooping	604
show ipv6 mld ssm-map	606
show ipv6 mld traffic	608
show ipv6 mrrib client	610
show ipv6 mrrib route	612
show ipv6 mroute	615
show ipv6 mtu	620

show ipv6 nd destination	622
show ipv6 nd on-link prefix	624
show ipv6 neighbors	625
show ipv6 ospf	630
show ipv6 ospf border-routers	634
show ipv6 ospf event	636
show ipv6 ospf graceful-restart	639
show ipv6 ospf interface	641
show ipv6 ospf request-list	646
show ipv6 ospf retransmission-list	648
show ipv6 ospf statistics	650
show ipv6 ospf summary-prefix	652
show ipv6 ospf timers rate-limit	653
show ipv6 ospf traffic	654
show ipv6 ospf virtual-links	658
show ipv6 pim anycast-RP	660
show ipv6 pim bsr	661
show ipv6 pim df	664
show ipv6 pim group-map	666
show ipv6 pim interface	668
show ipv6 pim join-prune statistic	670
show ipv6 pim limit	672
show ipv6 pim neighbor	673
show ipv6 pim range-list	675
show ipv6 pim topology	677
show ipv6 pim traffic	680
show ipv6 pim tunnel	682
show ipv6 policy	684
show ipv6 prefix-list	685
show ipv6 protocols	688
show ipv6 rip	690
show ipv6 routers	696
show ipv6 rpf	699
show ipv6 source-guard policy	701

show ipv6 spd 702
show ipv6 static 703
show ipv6 traffic 707
show key chain 710
show track 711
track 713
vrrp 715
vrrp description 716
vrrp preempt 717
vrrp priority 719
vrrp timers advertise 720
vrrs leader 722

PART V**IP マルチキャスト ルーティング 723**

CHAPTER 6**IP マルチキャスト ルーティング コマンド 725**

clear ip mfib counters 727
clear ip mroute 728
clear ip pim snooping vlan 730
debug condition vrf 731
debug ip pim 733
debug ipv6 pim 735
ip igmp filter 738
ip igmp max-groups 739
ip igmp profile 741
ip igmp snooping 743
ip igmp snooping last-member-query-count 744
ip igmp snooping querier 746
ip igmp snooping report-suppression 749
ip igmp snooping vlan mrouter 750
ip igmp snooping vlan static 751
ip multicast auto-enable 753
ip multicast-routing 754
ip pim accept-register 755

ip pim bsr-candidate	757
ip pim rp-candidate	759
ip pim send-rp-announce	761
ip pim snooping	763
ip pim snooping dr-flood	764
ip pim snooping vlan	765
ip pim spt-threshold	766
match message-type	767
match service-type	768
match service-instance	769
mrinfo	770
service-policy-query	772
service-policy	773
show ip igmp filter	774
show ip igmp profile	775
show ip igmp snooping	776
show ip igmp snooping groups	778
show ip igmp snooping mrouter	779
show ip igmp snooping querier	780
show ip pim autorp	782
show ip pim bsr-router	783
show ip pim bsr	784
show ip pim snooping	785
show ip pim tunnel	788
show platform software fed switch ip multicast	790

PART VI

レイヤ 2/3 793

CHAPTER 7

レイヤ 2/3 コマンド 795

channel-group	798
channel-protocol	802
clear l2protocol-tunnel counters	803
clear lacp	804
clear pagp	805

clear spanning-tree counters	806
clear spanning-tree detected-protocols	807
debug etherchannel	808
debug lacp	809
debug pagp	810
debug platform pm	811
debug platform udd	813
debug spanning-tree	814
instance (VLAN)	816
interface port-channel	818
l2protocol-tunnel	820
lacp fast-switchover	824
lacp max-bundle	826
lacp port-priority	827
lacp rate	829
lacp system-priority	830
loopdetect	831
name (MST)	834
pagp learn-method	835
pagp port-priority	837
port-channel	838
port-channel auto	839
port-channel load-balance	840
port-channel load-balance extended	842
port-channel min-links	844
rep admin vlan	845
rep block port	846
rep lsl-age-timer	848
rep lsl-retries	849
rep preempt delay	850
rep preempt segment	852
rep segment	854
rep stcn	856
revision	857

show dot1q-tunnel	859
show etherchannel	860
show interfaces rep detail	863
show l2protocol-tunnel	865
show lacp	867
show loopdetect	872
show pagp	873
show platform etherchannel	875
show platform pm	876
show rep topology	877
show spanning-tree	879
show spanning-tree mst	886
show udld	889
spanning-tree backbonefast	893
spanning-tree bpdufilter	894
spanning-tree bpduguard	896
spanning-tree bridge assurance	898
spanning-tree cost	900
spanning-tree etherchannel guard misconfig	902
spanning-tree extend system-id	904
spanning-tree guard	905
spanning-tree link-type	906
spanning-tree loopguard default	908
spanning-tree mode	909
spanning-tree mst	910
spanning-tree mst configuration	911
spanning-tree mst forward-time	913
spanning-tree mst hello-time	914
spanning-tree mst max-age	915
spanning-tree mst max-hops	916
spanning-tree mst pre-standard	917
spanning-tree mst priority	919
spanning-tree mst root	920
spanning-tree mst simulate pvst global	922

spanning-tree pathcost method	923
spanning-tree port-priority	924
spanning-tree portfast edge bpdudfilter default	926
spanning-tree portfast edge bpduguard default	928
spanning-tree portfast default	929
spanning-tree transmit hold-count	931
spanning-tree uplinkfast	933
spanning-tree vlan	934
switchport	937
switchport access vlan	939
switchport mode	940
switchport nonegotiate	943
switchport voice vlan	945
udld	948
udld port	950
udld reset	952
vlan dot1q tag native	953

PART VII**ネットワーク管理 955**

CHAPTER 8**ネットワーク管理コマンド 957**

cache	960
clear flow exporter	963
clear flow monitor	964
clear snmp stats hosts	966
collect	967
collect counter	969
collect flow sampler	970
collect interface	971
collect ipv4 destination	972
collect ipv4 source	973
collect timestamp absolute	975
collect transport tcp flags	976
collect routing next-hop address	977

datalink flow monitor	978
debug flow exporter	979
debug flow monitor	980
debug flow record	981
debug sampler	982
description	983
destination	984
dscp	986
event manager applet	987
export-protocol netflow-v9	991
export-protocol netflow-v5	992
exporter	993
fconfigure	994
flow exporter	995
flow monitor	996
flow record	997
ip wccp	998
ip flow monitor	1000
ipv6 flow monitor	1002
ipv6 deny echo reply	1004
match datalink dot1q priority	1005
match datalink dot1q vlan	1006
match datalink ethertype	1007
match datalink mac	1008
match datalink vlan	1010
match flow cts	1011
match flow direction	1012
match interface	1013
match ipv4	1014
match ipv4 destination address	1015
match ipv4 source address	1016
match ipv4 ttl	1017
match ipv6	1018
match ipv6 destination address	1019

match ipv6 hop-limit	1020
match ipv6 source address	1021
map platform-type	1022
match transport	1023
match transport icmp ipv4	1024
match transport icmp ipv6	1025
match platform-type	1026
mode random 1 out-of	1027
monitor capture (interface/control plane)	1028
monitor capture buffer	1030
monitor capture export	1031
monitor capture limit	1032
monitor capture start	1033
monitor capture stop	1034
monitor session destination	1035
monitor session filter	1039
monitor session source	1041
option	1044
record	1046
sampler	1047
show class-map type control subscriber	1048
show ip sla statistics	1049
show monitor	1051
show monitor capture	1053
show parameter-map type subscriber attribute-to-service	1055
show platform software fed switch ip wccp	1056
show platform software swspan	1058
show flow exporter	1060
show flow interface	1062
show flow monitor	1064
show flow record	1069
show sampler	1070
show snmp stats	1072
snmp ifmib ifindex persist	1074

snmp-server community	1075
snmp-server enable traps	1077
snmp-server enable traps bridge	1081
snmp-server enable traps bulkstat	1082
snmp-server enable traps call-home	1083
snmp-server enable traps cef	1084
snmp-server enable traps envmon	1085
snmp-server enable traps errdisable	1086
snmp-server enable traps flash	1087
snmp-server enable traps isis	1088
snmp-server enable traps license	1089
snmp-server enable traps mac-notification	1090
snmp-server enable traps ospf	1091
snmp-server enable traps pim	1093
snmp-server enable traps port-security	1094
snmp-server enable traps power-ethernet	1095
snmp-server enable traps snmp	1096
snmp-server enable traps storm-control	1097
snmp-server enable traps stpx	1098
snmp-server enable traps transceiver	1099
snmp-server enable traps vrfmib	1100
snmp-server enable traps vstack	1101
snmp-server engineID	1102
snmp-server group	1103
snmp-server host	1107
snmp-server manager	1112
snmp-server user	1113
snmp-server view	1118
source	1120
socket	1122
switchport mode access	1123
switchport voice vlan	1124
ttl	1125
transport	1126

template data timeout 1127

udp peek 1128

PART VIII

QoS 1129

CHAPTER 9

QoS コマンド 1131

auto qos classify 1132

auto qos trust 1135

auto qos video 1143

auto qos voip 1154

class 1168

class-map 1171

debug auto qos 1173

match (クラスマップ コンフィギュレーション) 1174

policy-map 1178

priority 1181

qos queue-softmax-multiplier 1183

queue-buffers ratio 1184

queue-limit 1185

random-detect cos 1187

random-detect cos-based 1189

random-detect dscp 1190

random-detect dscp-based 1192

random-detect precedence 1193

random-detect precedence-based 1195

service-policy (有線) 1196

set 1198

show auto qos 1204

show class-map 1206

show platform hardware fed switch 1207

show platform software fed switch qos 1211

show platform software fed switch qos qsb 1212

show policy-map 1215

show tech-support qos 1217

trust device 1219

PART IX

ルーティング 1221

CHAPTER 10

IP ルーティングコマンド 1223

accept-lifetime 1225

address-family ipv6 (OSPF) 1228

area nssa 1229

area virtual-link 1231

authentication (BFD) 1235

bfd 1236

bfd all-interfaces 1238

bfd check-ctrl-plane-failure 1239

bfd echo 1240

bfd slow-timers 1242

bfd template 1244

bfd-template single-hop 1245

default-information originate (OSPF) 1246

distance (OSPF) 1248

eigrp log-neighbor-changes 1251

eigrp log-neighbor-warnings 1253

ip authentication key-chain eigrp 1255

ip authentication mode eigrp 1256

ip bandwidth-percent eigrp 1258

ip cef load-sharing algorithm 1259

ip prefix-list 1260

ip hello-interval eigrp 1264

ip hold-time eigrp 1265

ip load-sharing 1267

ip network-broadcast 1268

ip ospf database-filter all out 1269

ip ospf name-lookup 1270

ip split-horizon eigrp 1271

ip summary-address eigrp	1272
ip route static bfd	1275
ipv6 route static bfd	1277
metric weights (EIGRP)	1279
neighbor description	1282
network (EIGRP)	1284
nsf (EIGRP)	1286
offset-list (EIGRP)	1288
redistribute (IP)	1290
redistribute (IPv6)	1299
redistribute maximum-prefix (OSPF)	1303
route-map	1305
router-id	1309
router eigrp	1310
router ospfv3	1311
send-lifetime	1312
show ip eigrp interfaces	1315
show ip eigrp neighbors	1318
show ip eigrp topology	1321
show ip eigrp traffic	1327
show ip ospf	1329
show ip ospf border-routers	1337
show ip ospf database	1338
show ip ospf interface	1348
show ip ospf neighbor	1352
show ip ospf virtual-links	1358
summary-address (OSPF)	1360
timers throttle spf	1362

PART X**セキュリティ 1365**

CHAPTER 11**セキュリティ 1367**

aaa accounting 1370

aaa accounting dot1x	1374
aaa accounting identity	1376
aaa authentication dot1x	1378
aaa new-model	1379
authentication host-mode	1381
authentication logging verbose	1383
authentication mac-move permit	1384
authentication priority	1386
authentication violation	1389
cisp enable	1391
clear errdisable interface vlan	1393
clear mac address-table	1394
confidentiality-offset	1396
crypto pki trustpool import	1397
debug aaa dead-criteria transaction	1400
debug umbrella	1402
delay-protection	1403
deny (MAC アクセス リスト コンフィギュレーション)	1404
device-role (IPv6 スヌーピング)	1408
device-role (IPv6 ND インスペクション)	1409
device-tracking (インターフェイス コンフィギュレーション)	1410
device-tracking (VLAN コンフィギュレーション)	1414
device-tracking binding	1417
device-tracking logging	1440
device-tracking policy	1444
device-tracking tracking	1460
device-tracking upgrade-cli	1466
dnscrypt (パラメータマップ)	1469
dot1x critical (グローバル コンフィギュレーション)	1470
dot1x logging verbose	1471
dot1x pae	1472
dot1x supplicant controlled transient	1473
dot1x supplicant force-multicast	1474

dot1x test eapol-capable	1475
dot1x test timeout	1476
dot1x timeout	1477
dtls	1480
enable password	1482
enable secret	1485
epm access-control open	1489
include-icv-indicator	1490
ip access-list	1491
ip access-list role-based	1494
ip admission	1495
ip admission name	1496
ip dhcp snooping database	1499
ip dhcp snooping information option format remote-id	1501
ip dhcp snooping verify no-relay-agent-address	1502
ip http access-class	1503
ip radius source-interface	1505
ip source binding	1507
ip ssh source-interface	1508
ip verify source	1509
ipv6 access-list	1511
ipv6 snooping policy	1513
key chain macsec	1514
key config-key password-encrypt	1515
key-server	1518
limit address-count	1520
local-domain (パラメータマップ)	1521
mab logging verbose	1522
mab request format attribute 32	1523
macsec-cipher-suite	1525
macsec network-link	1527
match (アクセス マップ コンフィギュレーション)	1528
mka pre-shared-key	1530
mka suppress syslogs sak-rekey	1531

parameter-map type regex	1532
parameter-map type umbrella global	1536
password encryption aes	1537
pattern (パラメータマップ)	1540
permit (MAC アクセス リスト コンフィギュレーション)	1543
protocol (IPv6 スヌーピング)	1547
radius server	1549
radius-server dead-criteria	1551
radius-server deadtime	1553
radius-server directed-request	1555
radius-server domain-stripping	1558
sak-rekey	1562
security level (IPv6 スヌーピング)	1564
send-secure-announcements	1565
server-private (RADIUS)	1567
server-private (TACACS+)	1570
show aaa clients	1572
show aaa command handler	1573
show aaa dead-criteria	1574
show aaa local	1576
show aaa servers	1578
show aaa sessions	1579
show authentication brief	1580
show authentication sessions	1583
show cisp	1586
show dot1x	1588
show eap pac peer	1590
show ip access-lists	1591
show ip dhcp snooping statistics	1594
show platform software dns-umbrella statistics	1597
show platform software umbrella switch F0	1598
show radius server-group	1600
show tech-support acl	1602

show tech-support identity	1607
show umbrella	1616
show vlan access-map	1618
show vlan filter	1619
show vlan group	1620
ssci-based-on-sci	1621
switchport port-security aging	1623
switchport port-security mac-address	1625
switchport port-security maximum	1628
switchport port-security violation	1630
tacacs server	1632
token (パラメータマップ)	1634
tracking (IPv6 スヌーピング)	1635
trusted-port	1637
umbrella	1638
use-updated-eth-header	1640
username	1642
vlan access-map	1648
vlan dot1Q tag native	1650
vlan filter	1651
vlan group	1652

PART XI

スタック マネージャおよびハイ アベイラビリティ	1653
--------------------------	------

CHAPTER 12

スタック マネージャおよびハイ アベイラビリティ コマンド	1655
main-cpu	1656
mode sso	1657
policy config-sync prc reload	1658
redundancy	1659
redundancy config-sync mismatched-commands	1660
redundancy force-switchover	1662
redundancy reload	1663
reload	1664
show redundancy	1665

[show redundancy config-sync](#) 1669
[show switch](#) 1671
[show switch stack-mode](#) 1677
[stack-mac persistent timer](#) 1678
[stack-mac update force](#) 1680
[standby console enable](#) 1681
[switch clear stack-mode](#) 1682
[switch switch-number role](#) 1683
[switch stack port](#) 1684
[switch priority](#) 1686
[switch provision](#) 1687
[switch renumber](#) 1689
[switch renumber](#) 1690

PART XII

[システム管理](#) 1691

CHAPTER 13

[システム管理コマンド](#) 1693

[arp](#) 1696
[boot](#) 1697
[boot system](#) 1698
[cat](#) 1699
[copy](#) 1700
[copy startup-config tftp:](#) 1701
[copy tftp: startup-config](#) 1702
[debug voice diagnostics mac-address](#) 1703
[debug platform condition feature multicast controlplane](#) 1704
[debug platform condition mac](#) 1706
[debug platform rep](#) 1708
[debug ilpower powerman](#) 1710
[delete](#) 1713
[dir](#) 1714
[exit](#) 1716
[factory-reset](#) 1717
[flash_init](#) 1720

help	1721
hostname	1722
install	1724
ip http banner	1738
ip http banner-path	1739
ip ssh bulk-mode	1740
l2 traceroute	1741
license air level	1742
license boot level	1744
license smart (グローバル コンフィギュレーション)	1747
license smart (特権 EXEC)	1758
license smart deregister	1764
license smart register idtoken	1766
license smart renew	1768
location	1770
location plm calibrating	1774
mgmt_init	1775
mkdir	1776
more	1777
no debug all	1778
rename	1779
request consent-token accept-response shell-access	1780
request consent-token generate-challenge shell-access	1781
request consent-token terminate-auth	1782
request platform software console attach switch	1783
reset	1785
rmdir	1786
sdm prefer	1787
service private-config-encryption	1788
set	1789
show avc client	1792
show bootflash:	1793
show debug	1796
show env xps	1797

show flow monitor	1801
show install	1806
show location	1808
show logging onboard switch uptime	1810
show license all	1813
show license authorization	1818
show license data translation	1823
show license eventlog	1824
show license history message	1826
show license reservation	1827
show license status	1828
show license summary	1837
show license tech	1840
show license udi	1848
show license usage	1850
show mac address-table	1854
show mac address-table move update	1859
show parser encrypt file status	1860
show platform integrity	1861
show platform software audit	1862
show platform software fed switch punt cause	1866
show platform software fed switch punt cpuq	1868
show platform software sl-infra	1871
show platform sudi certificate	1872
show running-config	1874
show sdm prefer	1880
show tech-support confidential	1882
show tech-support license	1883
show tech-support monitor	1885
show tech-support platform	1886
show tech-support platform evpn_vxlan	1890
show tech-support platform fabric	1893
show tech-support platform igmp_snooping	1897
show tech-support platform layer3	1900

[show tech-support platform mld_snooping](#) 1908
[show tech-support port](#) 1915
[show tech-support pvlan](#) 1918
[show version](#) 1919
[system env temperature threshold yellow](#) 1927
[tftp-server](#) 1929
[traceroute mac](#) 1931
[traceroute mac ip](#) 1934
[type](#) 1937
[unset](#) 1938
[version](#) 1940

CHAPTER 14
トレース 1941

[トレースについて](#) 1942
[トレースの概要](#) 1942
[トレースログの場所](#) 1942
[トレースログの命名規則](#) 1942
[ローテーションおよびスロットリングポリシー](#) 1943
[トレースレベル](#) 1943
[set platform software trace](#) 1945
[show platform software trace filter-binary](#) 1949
[show platform software trace message](#) 1950
[show platform software trace level](#) 1954
[request platform software trace archive](#) 1958
[request platform software trace rotate all](#) 1959
[request platform software trace filter-binary](#) 1960

PART XIII
VLAN 1961

CHAPTER 15
VLAN コマンド 1963

[clear vtp counters](#) 1964
[debug sw-vlan](#) 1965
[debug sw-vlan ifs](#) 1967

debug sw-vlan notification	1968
debug sw-vlan vtp	1970
private-vlan	1972
private-vlan mapping	1975
show interfaces private-vlan mapping	1977
show vlan	1978
show vtp	1982
switchport mode private-vlan	1989
switchport priority extend	1991
switchport trunk	1992
vlan	1995
vlan dot1q tag native	2003
vtp (グローバル コンフィギュレーション)	2004
vtp (インターフェイス コンフィギュレーション)	2010
vtp primary	2011

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



コマンドラインインターフェイスの使用

この章は、次の内容で構成されています。

- [コマンドラインインターフェイスの使用 \(2 ページ\)](#)

コマンドラインインターフェイスの使用

この章では、Cisco IOS コマンドラインインターフェイス (CLI) について説明し、CLI を使用してスイッチを設定する方法について説明します。

コマンドモードについて

Cisco IOS ユーザインターフェイスは、いくつかのモードに分かれています。使用可能なコマンドは、現在のモードによって異なります。各コマンドモードで使用できるコマンドのリストを取得するには、システムプロンプトで疑問符 (?) を入力します。

スイッチとのセッションを開始するときは、ユーザモード (別名ユーザ EXEC モード) が有効です。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえば、現在の設定ステータスを示す **show** コマンドや、カウンタまたはインターフェイスを消去する **clear** コマンドなど、ほとんどのユーザ EXEC コマンドは 1 回限りのコマンドです。スイッチの再起動時には、ユーザ EXEC コマンドは保存されません。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバルコンフィギュレーションモードを開始することもできます。

コンフィギュレーションモード (グローバル、インターフェイス、およびライン) を使用して、実行コンフィギュレーションを変更できます。コンフィギュレーションを保存するとこれらのコマンドは保存され、スイッチの再起動時に使用されます。各種のコンフィギュレーションモードにアクセスするには、まずグローバルコンフィギュレーションモードを開始する必要があります。グローバルコンフィギュレーションモードから、インターフェイスコンフィギュレーションモードおよびラインコンフィギュレーションモードを開始できます。

次の表に、主要なコマンドモード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。表の例では、ホスト名として *Switch* を使用しています。

表 1: コマンドモードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	Switch>	logout または quit を入力します。	このモードを使用して次の作業を行います。 <ul style="list-style-type: none"> • 端末の設定変更 • 基本テストの実行 • システム情報の表示

モード	アクセス方法	プロンプト	終了方法	モードの用途
特権 EXEC	ユーザ EXEC モードで、 enable コマンドを入力します。	デバイス#	終了するには、 disable と入力します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、 configure コマンドを入力します。	デバイス (config)#	終了して特権 EXEC モードに戻るには、 exit または end を入力するか、 Ctrl+Z を押します。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
VLAN コンフィギュレーション	グローバル コンフィギュレーションモードで、 vlan vlan-id コマンドを入力します。	デバイス (config-vlan)#	グローバル コンフィギュレーションモードに戻る場合は、 exit コマンドを入力します。 特権 EXEC モードに戻るには、 Ctrl+Z を押すか、 end を入力します。	このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTP モードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成してスイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーションモードで、 interface コマンドを入力し、インターフェイスを指定します。	デバイス (config-if)#	終了してグローバル コンフィギュレーションモードに戻るには、 exit を入力します。 特権 EXEC モードに戻るには、 Ctrl+Z を押すか、 end を入力します。	このモードを使用して、イーサネットポートのパラメータを設定します。
ライン コンフィギュレーション	グローバル コンフィギュレーションモードで回線を指定するには、 line vty または line console コマンドを入力します。	デバイス (config-line)#	終了してグローバル コンフィギュレーションモードに戻るには、 exit を入力します。 特権 EXEC モードに戻るには、 Ctrl+Z を押すか、 end を入力します。	このモードを使用して、端末回線のパラメータを設定します。

コマンドモードの詳細については、このリリースに対応するコマンドリファレンスガイドを参照してください。

ヘルプシステムについて

システムプロンプトに疑問符(?)を入力すると、各コマンドモードで使用できるコマンドの一覧が表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

表 2: ヘルプの概要

コマンド	目的
help	コマンドモードのヘルプシステムの簡単な説明を表示します。
<i>abbreviated-command-entry ?</i> デバイス# di? dir disable disconnect	特定のストリングで始まるコマンドのリストを表示します。
<i>abbreviated-command-entry <Tab></i> デバイス# sh conf<tab> デバイス# show configuration	特定のコマンド名を補完します。
? Switch> ?	特定のコマンドモードで使用可能なすべてのコマンドをリストします。
<i>command ?</i> Switch> show ?	コマンドに関連するキーワードを一覧表示します。
<i>command keyword ?</i> デバイス(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet	キーワードに関連する引数を一覧表示します。

コマンドの省略形

コマンドの先頭から、スイッチが特定のコマンドとして認識できる文字数だけを入力し、後は省略できます。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
デバイス# show conf
```

コマンドの **no** 形式および **default** 形式の概要

ほとんどのコンフィギュレーション コマンドには、**no** 形式もあります。**no** 形式は一般に、特定の機能または動作を無効にする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、インターフェイス コンフィギュレーション コマンド **no shutdown** を使用すると、インターフェイスのシャットダウンが取り消されます。キーワード **no** なしでコマンドを使用すると、無効にされた機能を再度有効にしたり、デフォルトで無効になっている機能を有効にしたりできます。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンド設定をデフォルトに戻します。ほとんどのコマンドはデフォルトで無効に設定されているため、**default** 形式を使用しても **no** 形式と同じ結果になります。ただし、デフォルトで有効に設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。このような場合、**default** コマンドはそのコマンドを有効にし、変数をそのデフォルト値に設定します。

CLI のエラーメッセージについて

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラーメッセージの一部を紹介します。

表 3: CLI の代表的なエラーメッセージ

エラーメッセージ	意味	ヘルプの表示方法
% Ambiguous command: "show con"	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符 (?) を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
% Incomplete command.	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符 (?) を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。

エラーメッセージ	意味	ヘルプの表示方法
% Invalid input detected at '^' marker.	コマンドの入力ミスです。間違っている箇所をキャレット (^) 記号で示しています。	疑問符 (?) を入力すると、そのコマンドモードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギングの使用法

スイッチの設定変更を記録して表示させることができます。Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザベースごとに変更内容をトラッキングできます。ログに記録されるのは、適用された各コンフィギュレーションコマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターンコードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。この通知を syslog に送信することも選択できます。



(注) CLI または HTTP の変更のみがログとして記録されます。

コマンド履歴の使用

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、10 のコマンドラインが履歴バッファに保存されます。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。これらの手順は任意です。

現在の端末セッションで保存されるコマンドライン数を変更するには、特権 EXEC モードで次のコマンドを入力します。

```
デバイス# terminal history [size number-of-lines]
```

指定できる範囲は 0 ~ 256 です。

特定の回線に関するすべてのセッションで保存されるコマンドライン数を設定するには、ラインコンフィギュレーション モードで次のコマンドを入力します。

```
デバイス(config-line)# history [size number-of-lines]
```

指定できる範囲は 0 ~ 256 です。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。これらの操作は任意です。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 4: コマンドの呼び出し

アクション	結果
Ctrl+P キーまたは↑キーを押します。	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N キーまたは↓キーを押します。	Ctrl+P または↑キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
show history デバイス(config)# help	特権 EXEC モードで、直前に入力したいくつかのコマンドを一覧表示します。表示されるコマンドの数は、 terminal history グローバル コンフィギュレーション コマンドおよび history ライン コンフィギュレーション コマンドの設定値によって制御されます。

コマンド履歴機能の無効化

コマンド履歴機能は、自動的に有効になっています。現在の端末セッションまたはコマンドラインで無効にできます。これらの手順は任意です。

現在の端末セッションでこの機能を無効にするには、**terminal no history** 特権 EXEC コマンドを使用します。

回線に関するセッションでコマンド履歴を無効にするには、**no history** ライン コンフィギュレーション コマンドを使用します。

編集機能の使用方法

ここでは、コマンドラインの操作に役立つ編集機能について説明します。

編集機能の有効化および無効化

拡張編集モードは自動的に有効になりますが、無効にする、再び有効にする、または特定の回線で拡張編集機能を使用できるように設定できます。これらの手順は任意です。

拡張編集モードをグローバルに無効にするには、ラインコンフィギュレーションモードで次のコマンドを入力します。

```
Switch (config-line)# no editing
```

現在の端末セッションで拡張編集モードを再び有効にするには、特権 EXEC モードで次のコマンドを入力します。

```
デバイス# terminal editing
```

特定の回線について拡張編集モードを再び設定するには、ラインコンフィギュレーションモードで次のコマンドを入力します。

```
デバイス(config-line)# editing
```

キーストロークによるコマンドの編集

このテーブルに、コマンドラインの編集に必要なキーストロークを示します。これらのキーストロークは任意です。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 5: キーストロークによるコマンドの編集

機能	キーストローク	目的
コマンドライン上を移動して、変更または訂正を行います。	Ctrl+B または左矢印キーを押します。	カーソルを 1 文字後退させます。
	Ctrl+F または右矢印キーを押します。	カーソルを 1 文字前進させます。
	Ctrl+A を押します。	カーソルをコマンドラインの先頭に移動します。
	Ctrl+E を押します。	カーソルをコマンドラインの末尾に移動します。
	Esc+B を押します。	カーソルを 1 単語後退させます。
	Esc+F を押します。	カーソルを 1 単語前進させます。
	Ctrl+T を押します。	カーソルの左にある文字を、カーソル位置の文字と置き換えます。

機能	キーストローク	目的
バッファからコマンドを呼び出し、コマンドラインにペーストします。最後に削除した 10 項目がバッファに保存されています。	Ctrl+Y を押します。	バッファ内の最新のエントリを呼び出します。
	Esc+Y を押します。	次のバッファエントリを呼び出します。 バッファには、最後に削除またはカットした 10 項目しか保存されません。Esc+Y を 11 回以上押すと、最初のバッファエントリに戻って表示されます。
不要なエントリを削除します。	Delete キーまたは Backspace キーを押します。	カーソルの左にある文字を消去します。
	Ctrl+D を押します。	カーソル位置にある文字を削除します。
	Ctrl+K を押します。	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
	Ctrl+U または Ctrl+X を押します。	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
	Ctrl+W を押します。	カーソルの左にある単語を削除します。
	Esc+D を押します。	カーソルの位置から単語の末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	Esc+C を押します。	カーソル位置のワードを大文字にします。
	Esc+L を押します。	カーソルの場所にある単語を小文字にします。
	Esc+U を押します。	カーソルの位置から単語の末尾までを大文字にします。

機能	キーストローク	目的
特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。	Ctrl+V または Esc+Q キーを押します。	
1行または1画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 (注) show コマンドの出力など、端末画面に一度に表示できない長い出力では、 More プロンプトが使用されます。 More プロンプトが表示された場合は、 Return キーおよび Space キーを使用してスクロールできます。	Return キーを押します。	1行下にスクロールします。
	Space キーを押します。	1画面分下にスクロールします。
スイッチから画面にメッセージが突然送られた場合に、現在のコマンドラインを再表示します。	Ctrl+L または Ctrl+R を押します。	現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で1行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは10文字分だけ左へシフトされます。コマンドラインの先頭から10文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、**Ctrl+B** キーまたは←キーを繰り返し押し続けます。コマンドラインの先頭に直接移動するには、**Ctrl+A** を押します。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次の例では、**access-list** グローバル コンフィギュレーション コマンドエントリが1行分よりも長くなっています。最初にカーソルが行末に達すると、その行は10文字分だけ左へシフトされ、再表示されます。ドル記号 (\$) は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び10文字分だけ左へシフトされます。

```
デバイス(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
デバイス(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
デバイス(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
デバイス(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わった後、Ctrl+A を押して全体の構文をチェックし、その後 Return キーを押してコマンドを実行してください。行末に表示されるドル記号 (\$) は、その行が右へスクロールされたことを表します。

```
デバイス(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。これらのコマンドの使用は任意です。

この機能を使用するには、**show** または **more** コマンドを入力した後、パイプ記号 (|)、**begin**、**include**、または **exclude** のいずれかのキーワード、および文字列（検索またはフィルタの条件）を指定します。

```
command | {begin | include | exclude} regular-expression
```

文字列では、大文字と小文字が区別されます。たとえば、**|exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

次の例では、*protocol* が使用されている行だけを出力するように指定する方法を示します。

```
デバイス# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

CLI のアクセス

CLI にはコンソール接続、Telnet、またはブラウザを使用することによってアクセスできます。

スイッチスタックおよびスイッチメンバインターフェイスは、アクティブスイッチを経由して管理します。スイッチごとにスイッチスタックメンバを管理することはできません。1 つまたは複数のスイッチメンバのコンソールポートまたはイーサネット管理ポートを経由してアクティブスイッチへ接続できます。アクティブスイッチへの複数の CLI セッションを使用する場合は注意が

必要です。1つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。



(注) スイッチスタックを管理する場合は、1つの CLI セッションを使用することを推奨します。

特定のスイッチメンバポートを設定する場合は、CLI コマンドインターフェイス表記にスイッチメンバ番号を含めてください。

特定のスイッチメンバをデバッグする場合は、**session stack-member-number** 特権 EXEC コマンドでアクティブスイッチからアクセスできます。スイッチメンバ番号は、システムプロンプトに追加されます。たとえば、**Switch-2#** はスイッチメンバ 2 の特権 EXEC モードのプロンプトであり、アクティブスイッチのシステムプロンプトは **Switch** です。特定のスタックメンバへの CLI セッションで使用できるのは、**show** コマンドと **debug** コマンドに限ります。

コンソール接続または Telnet による CLI アクセス

CLI にアクセスするには、スイッチのハードウェア インストールガイドに記載されている手順で、スイッチのコンソールポートに端末または PC を接続するか、または PC をイーサネット管理ポートに接続して、スイッチの電源をオンにする必要があります。

CLI アクセスはスイッチのセットアップの前に使用できます。スイッチが設定された後は、リモート Telnet セッションまたは SSH クライアントで CLI にアクセスできます。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチのコンソールポートに管理ステーションまたはダイヤルアップ モデムを接続するか、イーサネット管理ポートに PC を接続します。コンソールポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェアインストールガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化セキュア シェル (SSH) パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブルシークレットパスワードを設定しておくことも必要です。

スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソールポート、イーサネット管理ポート、Telnet セッション、または SSH セッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。



第 1 部

Cisco SD-Access

- [Cisco SD-Access コマンド](#), on page 15



Cisco SD-Access コマンド

- broadcast-underlay, on page 17
- database-mapping, on page 18
- dynamic-eid, on page 20
- eid-record-provider, on page 21
- eid-record-subscriber, on page 22
- eid-table, on page 23
- encapsulation, on page 25
- etr, on page 26
- etr map-server, on page 27
- extranet, on page 29
- first-packet-petr, on page 30
- instance-id, on page 32
- ip pim lisp core-group-range, on page 33
- ip pim lisp transport multicast, on page 34
- ip pim rp-address, on page 35
- ip pim sparse mode, on page 36
- ipv4 multicast multitopology, on page 37
- ip pim ssm, on page 38
- itr, on page 39
- itr map-resolver, on page 40
- locator default-set, on page 41
- locator-set, on page 42
- map-cache , on page 43
- map-cache extranet, on page 44
- prefix-list, on page 45
- route-import database, on page 46
- service, on page 48
- show lisp instance-id ipv4 database, on page 49
- show lisp instance-id ipv6 database, on page 51
- show lisp instance-id ipv4 map-cache, on page 52
- show lisp instance-id ipv6 map-cache, on page 58
- show lisp instance-id ipv4 server, on page 60
- show lisp instance-id ipv6 server, on page 62

- [show lisp instance-id ipv4 statistics](#), on page 63
- [show lisp instance-id ipv6 statistics](#), on page 64
- [show lisp prefix-list](#), on page 65
- [show lisp session](#), on page 66
- [use-petr](#), on page 67

broadcast-underlay

LISP ネットワーク内にアンダーレイを設定し、マルチキャストグループを使用してカプセル化されたブロードキャストパケットとリンクローカルマルチキャストパケットを送信するには、**service** サブモードで **broadcast-underlay** コマンドを使用します。

[no] **broadcast-underlay** *multicast-ip*

Syntax Description	<i>multicast-ip</i> カプセル化されたブロードキャストパケットの送信に使用するマルチキャストグループの IP アドレス				
Command Default	なし				
Command Modes	LISP サービスイーサネット (router-lisp-inst-serv-eth)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1c</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。				

Usage Guidelines このコマンドを使用して、LISP ネットワーク内のファブリック エッジ ノード上でブロードキャスト機能をイネーブルにします。このコマンドは必ず **router-lisp-service-ethernet** モードまたは **router-lisp-instance-service-ethernet** モードで使用してください。

ブロードキャスト機能を削除するには、このコマンドの **no** 形式を使用します。

次に、ファブリック エッジ ノードでブロードキャストを設定する例を示します。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ethernet
device(config-router-lisp-inst-serv-eth)#eid-table vlan 250
device(config-router-lisp-inst-serv-eth)#broadcast-underlay 225.1.1.1
device(config-router-lisp-inst-serv-eth)#database-mapping mac locator-set rloc2
device(config-router-lisp-inst-serv-eth)#exit-service-ethernet
```

database-mapping

IPv4 または IPv6 のエンドポイント識別子からルーティングロケータ（EID-to-RLOC）のマッピング関係および Locator/ID Separation Protocol（LISP）の関連トラフィックポリシーを設定するには、LISP EID テーブル コンフィギュレーション モードで **database-mapping** コマンドを使用します。設定したデータベースのマッピングを削除するには、このコマンドの **no** 形式を使用します。

```
[ no ] database-mapping eid-prefix / prefix-length { locator-set RLOC-name [ proxy ] |
ipv6-interface interface-name | ipv4-interface interface-name | auto-discover-rlocs | limit }
```

Syntax Description

eid-prefix / prefix-length	ルータによってアドバタイズされる IPv4 または IPv6 のエンドポイント識別子のプレフィックスとその長さを指定します。
locator-set RLOC-name	eid-prefix に指定された値に関連付けられたルーティングロケータ（RLOC）を指定します。
proxy	スタティック プロキシデータベース マッピングの設定を有効にします。
ipv4 interface interface-name	EID プレフィックスの RLOC として使用するインターフェイスの IPv4 アドレスと名前を指定します。
ipv6 interface interface-name	EID プレフィックスの RLOC として使用するインターフェイスの IPv6 アドレスと名前を指定します。
auto-discover-rlocs	ETR LISP サイトが複数の xTR を使用し、各 xTR が DHCP の既知のロケータを使用するように設定されている、または自身のロケータを使用するように設定されている場合、出力トンネルルータ（ETR）と入力トンネルルータ（ITR）の両方として機能するように設定されている ETR LISP サイトのすべてのルータ（このようなルータは xTR と呼ばれる）のロケータを検出するように出力トンネルルータ（ETR）を設定します。
limit	ローカル EID プレフィックスデータベースの最大サイズを指定します。

Command Default

LISP データベース エントリは定義されません。

Command Modes

LISP インスタンスサービス（router-lisp-instance-service）

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

LISP インスタンス サービス コンフィギュレーションモードでは、**database-mapping** コマンドは、指定の IPv4 または IPv6 の EID プレフィックスブロックの LISP データベースパラメータを設定します。ロケータは、サイトに関連付けられた EID プレフィックスの RLOC アドレスとして使用さ

れているインターフェイスの IPv4 アドレスまたは IPv6 アドレスですが、インターフェイスのルーブバック アドレスとしても使用できます。

LISP サイトに同じ EID プレフィックスブロックに関連付けられているロケータが複数ある場合、複数の **database-mapping** コマンドを使用して、特定の EID プレフィックスブロックのすべてのロケータを設定できます。

マルチサイトのシナリオでは、LISP ボーダーノードが接続されているサイトの EID を中継マップサーバ上でアドバタイズしてサイトトラフィックを誘導します。これを行うには、内部ボーダーからルートを取得し、中継サイトマップサーバにプロキシを登録する必要があります。

database-mapping eid-prefix locator-set RLOC-name proxy コマンドを使用すると、スタティックプロキシデータベースマッピングを設定できます。

次に、外部ボーダーの EID コンフィギュレーションモードで、locator-set、RLOC を使用して eid-prefix をマッピングする例を示します。



Note locator-set RLOC がすでに設定されていることが必要です。

```
device(config)# router lisp
device(config-router-lisp)# instance-id 3
device(config-router-lisp-inst)# service ipv4
device(config-router-lisp-inst-serv-ipv4)#eid-table vrf red
device(config-router-lisp-inst-serv-ipv4-eid-table)# database-mapping 172.168.0.0/16
locator-set RLOC proxy
device(config-router-lisp-inst-serv-ipv4-eid-table)# database-mapping 173.168.0.0/16
locator-set RLOC proxy
device(config-router-lisp-inst-serv-ipv4-eid-table)# map-cache 0.0.0.0/0 map-request
device(config-router-lisp-inst-serv-ipv4-eid-table)#exit
device(config-router-lisp-inst-serv-ipv4)#
```

Related Commands

コマンド	説明
eid-table vrf <i>vrf-name</i>	instance-service のインスタンス化を、仮想ルーティングおよび転送 (VRF) テーブル、またはエンドポイント ID アドレス空間に到達可能なデフォルトのテーブルと関連付けます。

dynamic-eid

ダイナミックエンドポイント識別子（EID）のポリシーを作成し、xTRでdynamic-eid コンフィギュレーション モードを開始するには、**dynamic-eid** コマンドを使用します。

dynamic-eid *eid-name*

Syntax Description

eid-name *eid-name* が存在する場合は、*eid-name* コンフィギュレーションモードを開始します。または、*eid-name* という名前の新しい dynamic-eid ポリシーが作成され、dynamic-eid コンフィギュレーションモードを開始します。

Command Default

LISP dynamic-eid ポリシーは設定されません。

Command Modes

LISP EID テーブル (router-lisp-eid-table)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

LISP モビリティを設定するには、**lisp mobility** インターフェイスコマンドで参照可能なダイナミック EID ローミング ポリシーを作成します。**dynamic-eid** コマンドが入力されると、参照先の LISP ダイナミック EID ポリシーが作成され、ダイナミック EID コンフィギュレーションモードが開始します。このモードでは、参照先の LISP ダイナミック EID ポリシーに関連付けられているすべての属性を入力できます。ダイナミック EID ポリシーを設定する場合、EID から RLOC へのダイナミックなマッピング関係と、それに関連するトラフィック ポリシーを指定する必要があります。

Related Commands

コマンド D	説明
lisp mobility	ITR のインターフェイスを LISP モビリティ（ダイナミック EID ローミング）に参加するように設定します。

eid-record-provider

プロバイダーインスタンスにエクストラネット ポリシー テーブルを定義するには、lisp-extranet モードで **eid-record-provider** コマンドを使用します。

[no] **eid-record-provider instance-id** *instance id* {*ipv4 address prefix* | *ipv6 address prefix*} **bidirectional**

Syntax Description

instance-id *instance id* エクストラネット プロバイダー ポリシーを適用する LISP インスタンスのインスタンス ID。

ipv4 address prefix リークする IPv4 EID プレフィックスを a.b.c.d/nn 形式で指定して定義します。

ipv6 address prefix リークする IPv6 EID プレフィックスを、X:X:X:X::X/<0-128> 形式で指定したプレフィックスで定義します。

bidirectional プロバイダーとサブスクリバ EID プレフィックス間のエクストラネット通信が双方向であることを指定します。

Command Default

なし

Command Modes

router-lisp-extranet

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

eid-record-provider 設定を無効にするには、このコマンドの **no** 形式を使用します。

```
device(config)#router lisp
device(config-router-lisp)#extranet ext1
device(config-router-lisp-extranet)#eid-record-provider instance-id 5000 10.0.0.0/8
bidirectional
device(config-router-lisp-extranet)#eid-record-subscriber instance-id 1000 3.0.0.0/24
bidirectional
```

eid-record-subscriber

サブスクリバインスタンスにエクストラネットポリシーテーブルを定義するには、lisp-extranet モードで **eid-record-subscriber** コマンドを使用します。

[no] eid-record-subscriber instance-id instance id {ipv4 address prefix | ipv6 address prefix} bidirectional

Syntax Description	instance-id instance id エクストラネットプロバイダーポリシーを適用する LISP インスタンスのインスタンス ID。
	ipv4 address prefix リークする IPv4 EID プレフィックスを a.b.c.d/nn 形式で指定して定義します。
	ipv6 address prefix リークする IPv6 EID プレフィックスを、X:X:X:X::X/<0-128> 形式で指定したプレフィックスで定義します。
	bidirectional プロバイダーとサブスクリバ EID プレフィックス間のエクストラネット通信が双方向であることを指定します。

Command Default なし

Command Modes LISP エクストラネット (router-lisp-extranet)

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines eid-record-subscriber 設定を無効にするには、このコマンドの **no** 形式を使用します。

```
device(config)#router lisp
device(config-router-lisp)#extranet ext1
device(config-router-lisp-extranet)#eid-record-provider instance-id 5000 10.0.0.0/8
bidirectional
device(config-router-lisp-extranet)#eid-record-subscriber instance-id 1000 3.0.0.0/24
bidirectional
device(config-router-lisp-extranet)#eid-record-subscriber instance-id 2000 20.20.0.0/8
bidirectional
```

eid-table

eid-table コマンドは、instance-service のインスタンス化を、仮想ルーティングおよび転送（VRF）テーブル、またはエンドポイント ID アドレス空間に到達可能なデフォルトのテーブルと関連付けます。

```
[no] eid-table {vrf-name | default | vrf vrf-name}
```

Syntax Description	default 設定した instance-service と関連付けるためのデフォルト（グローバル）のルーティングテーブルを選択します。
	vrf vrf-name 設定したインスタンスと関連付けるための名前付き VRF テーブルを選択します。

Command Default デフォルトの VRF は、instance-id 0 に関連付けられます。

Command Modes router-lisp-instance-service

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines このコマンドは instance-service モードでのみ使用します。

レイヤ 3（service ipv4/service ipv6）の場合、VRF テーブルが instance-service に関連付けられます。レイヤ 2（service ethernet）の場合、VLAN が instance-service に関連付けられます。



Note レイヤ 2 の場合、eid-table を設定する前に VLAN を定義しておきます。
レイヤ 3 の場合、eid-table を設定する前に VRF テーブルを定義しておきます。

次の例では、vrf-table という名前の VRF を使用してトラフィックをセグメント化するように XTR が設定されています。vrf-table に関連付けられている EID プレフィックスがインスタンス ID 3 に接続されます。

```
device(config)#vrf definition vrf-table
device(config-vrf)#address-family ipv4
device(config-vrf-af)#exit
device(config-vrf)#exit
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#eid-table vrf vrf-table
```

次の例では、Vlan10 という名前の VLAN に関連付けられている EID プレフィックスがインスタンス ID 101 に接続されています。

```
device(config)#interface Vlan10
device(config-if)#mac-address ba25.cdf4.ad38
device(config-if)#ip address 10.1.1.1 255.255.255.0
device(config-if)#end
device(config)#router lisp
device(config-router-lisp)#instance-id 101
device(config-router-lisp-inst)#service ethernet
device(config-router-lisp-inst-serv-ethernet)#eid-table Vlan10
device(config-router-lisp-inst-serv-ethernet)#database-mapping mac locator-set set
device(config-router-lisp-inst-serv-ethernet)#exit-service-etherne
device(config-router-lisp-inst)#exit-instance-id
```

encapsulation

LISP ネットワーク内でデータパケットのカプセル化のタイプを設定するには、service モードで **encapsulation** コマンドを使用します。

[no] **encapsulation** {vxlan | lisp}

Syntax Description

encapsulation vxlan VXLAN ベースのカプセル化を指定します。

encapsulation lisp LISP ベースのカプセル化を指定します。

Command Default

なし

Command Modes

LISP サービス IPv4 (router-lisp-serv-ipv4)

LISP サービス IPv6 (router-lisp-serv-ipv6)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

encapsulation vxlan コマンドを service ethernet モードで使用して、レイヤ2 パケットをカプセル化します。**encapsulation lisp** コマンドを service ipv4 モードまたは service ipv6 モードで使用して、レイヤ3 パケットをカプセル化します。

パケットのカプセル化を削除するには、このコマンドの **no** 形式を使用します。

次に、データ カプセル化に xTR を設定する例を示します。

```
device(config)#router lisp
device(config-router-lisp)#service ipv4
device(config-router-lisp-serv-ipv4)#encapsulation vxlan
device(config-router-lisp-serv-ipv4)#map-cache-limit 200
device(config-router-lisp-serv-ipv4)#exit-service-ipv4
```

etr

出力トンネルルータ（ETR）としてデバイスを設定するには、instance-service モードまたは service サブモードで **etr** コマンドを使用します。

[no] **etr**

Command Default デフォルトでは、デバイスは ETR として設定されていません。

Command Modes router-lisp-instance-service
router-lisp-service

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines デバイスをイネーブルにして ETR 機能を実行するには、このコマンドを使用します。

ETR 機能を削除するには、このコマンドの **no** 形式を使用します。

ETR として設定されたルータも通常は **database-mapping** コマンドで設定されているため、ETR はどのエンドポイント ID（EID）のプレフィックスブロックと対応するロケータが LISP サイトに使用されているかを認識しています。さらに、ETR は **etr map-server** コマンドを使用してマップサーバに登録されるように設定するか、または **map-cache** コマンドを使用してスタティック LISP EID-to-RLOC（EID から RLOC）ロケータを使用するように設定する必要があります。

次に、ETR としてデバイスを設定する例を示します。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#etr
```

etr map-server

EID の設定時に出力トンネルルータ（ETR）を使用するようにマップサーバを設定するには、instance モードまたは instance-service モードで **etr map-server** コマンドを使用します。マップサーバの設定済みのロケータアドレスを削除するには、このコマンドの **no** 形式を使用します。

etr map-server *map-server-address* {**key** [0|6|7] *authentication-key* | **proxy-reply** }

Syntax Description	<i>map-server-address</i> マップサーバのロケータアドレス。
key	キータイプを指定します。
0	クリアテキストとしてパスワードが入力されることを示します。
6	そのパスワードは AES 暗号化形式であることを示します。
7	暗号化が弱いパスワードであることを示します。
<i>authentication-key</i>	map-register メッセージのヘッダーに含まれる SHA-1 HMAC ハッシュの計算に使用されるパスワード。
proxy-reply	ETR の代わりにマップサーバが map-request に応答することを指定します。
Command Default	なし
Command Modes	LISP インスタンスサービス (router-lisp-inst-serv) LISP サービス (router-lisp-serv)
Command History	リリース 変更内容 Cisco IOS XE Gibraltar 16.11.1c このコマンドが導入されました。

Usage Guidelines ETR がその EID を登録するマップサーバのロケータを設定するには、**etr map-server** コマンドを使用します。コマンド構文内の認証キー引数が、（**map-register** メッセージのヘッダーに含まれる）SHA-1 HMAC ハッシュに使用されるパスワードです。SHA 1 HMAC で使用されるパスワードは暗号化されていない（クリアテキスト）形式か、または暗号化された形式で入力されます。暗号化されていないパスワードを入力するには、**0** を指定します。AES 暗号化パスワードを入力するには、**6** を指定します。

マップサーバ機能を削除するには、このコマンドの **no** 形式を使用します。

次に、ETR で **map-requests** に応答するために、2.1.1.6 にあるマップサーバをプロキシとして機能するように設定する例を示します。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
```

```
device(config-router-lisp-inst-serv-ipv4)#etr map-server 2.1.1.6 key foo
device(config-router-lisp-inst-serv-ipv4)#etr map-server 2.1.1.6 proxy-reply
```

extranet

LISP ネットワーク内で VRF 間通信をイネーブルにするには、MSMR で、**extranet** コマンドを LISP コンフィギュレーションモードで使用します。

extranet *name-extranet*

Syntax Description	<i>name-extranet</i> 作成したエクストラネットの名前を指定します。
---------------------------	---

Command Default	なし
------------------------	----

Command Modes	LISP (router-lisp)
----------------------	--------------------

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

```
device(config)#router lisp
device(config-router-lisp)#extranet ext1
device(config-router-lisp-extranet)#
```

first-packet-petr

最初のパケット（およびmap-cacheが解決されるまでの後続のパケット）の損失を防ぐには、マップサーバー上で、LISP-service または LISP-instance-service コンフィギュレーション モードにより **first-packet-petr** コマンドを使用します。このコマンドの設定を無効にするには、このコマンドの **no** 形式を使用します。

このコマンドを設定すると、ファブリックエッジデバイスから送信された最初のパケットでも、使用可能な first-packet-handler ボーダーを介して宛先に到達します。

```
[no] first-packet-petr remote-locator-set fpetr-RLOC
```

Syntax Description	remote-locator-set <i>fpetr-RLOC</i>	リモートロケータセットを指定します。リモートロケータセットは、外部ネットワーク、サイト間のネットワーク、リモートサイト、またはローカルサイトを介してデータセンターに接続するリモートデバイスの IP アドレスのセットです。
Command Default	なし。	
Command Modes	LISP-instance-service LISP-service	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが追加されました。
Usage Guidelines	<p>ITR またはファブリックエッジデバイスは、ローカル MSMR から宛先の EID の到達可能性を学習するまで、最初に送信されたパケットをドロップします。最初のパケットのドロップを防ぐには、ローカル MSMR で first-packet-petr コマンドを設定します。</p> <p>ローカルマップサーバーで first-packet-petr コマンドを設定し、ファブリックエッジが起動して 0/0 マップキャッシュエントリを解決したときに、最初のパケット転送 RLOC を取得するようにします。</p> <p>MSMR は、外部ネットワーク（インターネットなど）への接続要求を受信すると、まず外部境界の可用性をチェックします。マップサーバーは、デフォルト ETR ボーダーまたはインターネットサービス提供ボーダーが見つからない場合、first-packet-petr コマンドで設定されたリモート RLOC で応答します。</p>	



Note **first-packet-petr** コマンドは、ファブリックサイト内のコントロールプレーンでのみ設定できません。このコマンドは、中継サイトのコントロールプレーンでは設定できません。

例

次の例では、最初にリモートロータセットを定義し、リモートRLOCをfirst-packet-petrコマンドに関連付けます。

```
Device(config)#router lisp
Device(config-router-lisp)#remote-locator-set fpetr
Device(config-router-lisp-remote-locator-set)#23.23.23.23 priority 1 weight 1
Device(config-router-lisp-remote-locator-set)#24.24.24.24 priority 1 weight 1
Device(config-router-lisp-remote-locator-set)#exit-remote-locator-set

Device(config-router-lisp)#service ipv4
Device(config-lisp-srv-ipv4)#first-packet-petr remote-locator-set fpetr
Device(config-lisp-srv-ipv4)#map-server
Device(config-lisp-srv-ipv4)#map-resolver
Device(config-lisp-srv-ipv4)#exit-service-ipv4
Device(config-router-lisp)#
```

設定された動作は、サービス ipv4 の下のすべてのインスタンスに継承されます。

特定のインスタンスの動作を上書きするには、そのインスタンスに対してfirst-packet-petrコマンドを設定します。次の例では、インスタンス101がfirst-packet-petrコマンドを無効にします。

```
Device(config-router-lisp)#instance-id 101
Device(config-router-lisp-inst)#service ipv4
Device(config-router-lisp-inst-service-ipv4)#no first-packet-petr remote-locator-set
Device(config-router-lisp-inst-service-ipv4)#exit-service-ipv4
```

instance-id

router-lisp コンフィギュレーション モードで LISP EID インスタンスを作成して、instance-id サブモードを開始するには、**instance-id** コマンドを使用します。

instance-id *iid*

Command Default なし

Command Modes LISP (router-lisp)

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines LISP EID インスタンスを使用して複数のサービスをグループ化するには、instance-id コマンドを使用します。

この instance-id での設定が、下位のすべてのサービスに適用されます。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#
```

ip pim lisp core-group-range

LISP サブインターフェイスにおける Protocol Independent Multicast (PIM) 送信元特定マルチキャスト (SSM) のアドレスのコア範囲を設定するには、インターフェイスコンフィギュレーションモードで **ip pim lisp core-group-range** コマンドを使用します。SSM アドレス範囲を削除するには、このコマンドの **no** 形式を使用します。

[no] **ip pim lisp core-group-range** *start-SSM-address range-size*

Syntax Description

start-SSM-address 範囲内の最初の SSM IP アドレスを指定します。

number-of-groups グループ範囲のサイズを指定します。

Command Default

アドレスのコア範囲が設定されていない場合、デフォルトではグループ範囲 232.100.100.1 ~ 232.100.100.255 が割り当てられます。

Command Modes

LISP インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE 16.9.1	このコマンドが導入されました。

Usage Guidelines

ネイティブマルチキャストトランスポートは、アンダーレイまたはコアで PIM SSM のみをサポートします。マルチキャストトランスポートでは、グループ化メカニズムを使用して、エンドポイント識別子 (EID) エントリを RLOC 空間 SSM グループエントリにマッピングします。デフォルトでは、LISP インターフェイスでマルチキャストトラフィックを転送するアドレスの SSM 範囲としてグループ範囲 232.100.100.1 ~ 232.100.100.255 が使用されます。LISP インターフェイスにおける IP アドレスの SSM コアグループ範囲を手動で変更するには、**ip pim lisp core-group-range** コマンドを使用します。

次の例では、マルチキャストトラフィックに使用するコアのアドレスの SSM 範囲として 232.0.0.1 から始まる 1000 個の IP アドレスのグループを定義しています。

```
Device(config)#interface LISP0.201
Device(config-if)#ip pim lisp core-group-range 232.0.0.1 1000
```

ip pim lisp transport multicast

LISP インターフェイスおよびサブインターフェイスのトランスポートメカニズムとしてマルチキャストをイネーブルにするには、LISP インターフェイス コンフィギュレーション モードで **ip pim lisp transport multicast** コマンドを使用します。LISP インターフェイスのトランスポートメカニズムとしてマルチキャストをディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] ip pim lisp transport multicast

構文の説明

このコマンドにはキーワードまたは引数はありません。

Command Default

このコマンドが設定されていない場合は、ヘッドエンド レプリケーションがマルチキャストに使用されます。

Command Modes

LISP インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE 16.9.1	このコマンドが導入されました。

例

次に、LISP インターフェイスのトランスポートメカニズムとしてマルチキャストを設定する例を示します。

```
Device(config)#interface LISP0
Device(config-if)#ip pim lisp transport multicast
```

Related Commands

コマンド	説明
ip multicast routing	IP マルチキャストルーティングまたはマルチキャスト分散スイッチングをイネーブルにします。

ip pim rp-address

特定グループの Protocol-Independent Multicast (PIM) ランデブーポイント (RP) のアドレスを設定するには、グローバル コンフィギュレーション モードで **ip pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
[no] ip pim [vrfvrf-name] rp-address rp-address [access-list]
```

Syntax Description	
vrf	(任意) バーチャルプライベート ネットワーク (VPN) ルーティングおよび転送 (VRF) インスタンスを指定します。
vrf-name	(任意) VRF に割り当てられた名前。
rp-address	PIM RP になるルータの IP アドレス。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。
access-list	(任意) RP を使用するマルチキャストグループを定義するアクセスリストの名前または番号。

Command Default なし

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE 16.8.1s	このコマンドが導入されました。

Usage Guidelines スパースモードまたは双方向モードで動作するマルチキャストグループの RP アドレスをステータックに定義するには、**ip pim rp-address** コマンドを使用します。

複数のグループに単一の RP を使用するように Cisco IOS ソフトウェアを設定できます。アクセスリストで指定されている条件によって、RP を使用できるグループが決定されます。アクセスリストが設定されていない場合は、すべてのグループに RP が使用されます。PIM ルータは複数の RP を使用できますが、グループごとに 1 つのみです。

次に、すべてのマルチキャストグループに対して PIM RP アドレスを 185.1.1.1 に設定する例を示します。

```
Device(config)#ip pim rp-address 185.1.1.1
```

ip pim sparse mode

インターフェイスの Protocol Independent Multicast (PIM) のスパース動作モードをイネーブルにするには、インターフェイス コンフィギュレーションモードで **ip pim sparse-mode** コマンドを使用します。スパース動作モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] ip pim sparse mode{

構文の説明

このコマンドにはキーワードまたは引数はありません。

Command Default

なし

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE 16.8.1s	このコマンドが導入されました。

Usage Guidelines

NetFlow **collect** コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。**nonkey** フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。**nonkey** フィールドの値の変更によって新しいフローが作成されることはありません。

次に、**PIM** スパース動作モードを設定する例を示します。

```
Device(config)#interface Loopback0
Device(config-if)#ip address 170.1.1.1 255.255.255.0
Device(config-if)#ip pim sparse-mode
```

Related Commands

コマンド	説明
ip multicast routing	IP マルチキャストルーティングまたはマルチキャスト分散スイッチングをイネーブルにします。

ipv4 multicast multitopology

IP マルチキャストルーティングのマルチキャスト固有 RPF トポロジのサポートをイネーブルにするには、VRF コンフィギュレーションモードで **ipv4 multicast multitopology** コマンドを使用します。マルチキャスト固有 RPF トポロジのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] **ipv4 multicast multitopology**

構文の説明

このコマンドには引数またはキーワードはありません。

Command Default

なし

Command Modes

VRF コンフィギュレーション (config-vrf)

Command History

リリース	変更内容
Cisco IOS XE 16.8.1s	このコマンドが導入されました。
Cisco IOS XE Fuji 16.8.1a	

次に、マルチキャスト固有 RPF トポロジを設定する例を示します。

```
Device(config)#vrf definition VRF1
Device(config-vrf)#ipv4 multicast multitopology
```

ip pim ssm

IP マルチキャストアドレスの送信元特定マルチキャスト（SSM）範囲を定義するには、グローバル コンフィギュレーション モードで **ip pim ssm** コマンドを使用します。SSM 範囲をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
[no] ip pim [vrfvrf-name] ssm {default | range access-list}
```

Syntax Description	vrf	(任意) バーチャルプライベートネットワーク (VPN) ルーティングおよび転送 (VRF) インスタンスを指定します。
	vrf-name	(任意) VRF に割り当てられた名前。
	range access-list	SSM 範囲を定義する標準 IP アクセスリストの番号または名前を指定します。
	default2	SSM 範囲アクセスリストを 232/8 に定義します。

Command Default なし

Command Modes グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE 16.8.1s	このコマンドが導入されました。

Usage Guidelines IP マルチキャストアドレスの SSM 範囲を **ip pim ssm** コマンドで定義すると、SSM 範囲内で承認および発信される Multicast Source Discovery Protocol (MSDP) の送信元アクティブ (SA) メッセージはなくなります。

次に、IP マルチキャストアドレスの **SSM** 範囲をデフォルトに設定する例を示します。

```
Device(config)#ip pim ssm default
```

Related Commands	コマンド	説明
	ip multicast routing	IP マルチキャストルーティングまたはマルチキャスト分散スイッチングをイネーブルにします。

itr

入力トンネルルータ (ITR) としてデバイスを設定するには、`service` サブモードまたは `instance-service` モードで `itr` コマンドを使用します。

[`no`] `itr`

Command Default

デフォルトでは、デバイスは ITR として設定されません。

Command Modes

LISP インスタンスサービス (`router-lisp-instance-service`)

LISP サービス (`router-lisp-service`)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

デバイスをイネーブルにして ITR 機能を実行するには、このコマンドを使用します。

ITR 機能を削除するには、このコマンドの `no` 形式を使用します。

ITR として設定されたデバイスは、LISP 対応サイト宛のすべてのトラフィックの EID から RLOC へのマッピングの検出に役立ちます。

次に、ITR としてデバイスを設定する例を示します。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#itr
```

itr map-resolver

map-request の送信時に入力トンネルルータ（ITR）が使用するマップリゾルバとしてデバイスを設定するには、service サブモードまたは instance-service モードで **itr map-resolver** コマンドを使用します。

```
[no] itr [map-resolver map-address] prefix-list prefix-list-name
```

Syntax Description	map-resolver map-address ITR で、マップ要求の送信用にマップリゾルバアドレスを設定します。				
	prefix-list prefix-list-name 使用するプレフィックスリストを指定します。				
Command Default	なし				
Command Modes	router-lisp-instance-service				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1c</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。				
Usage Guidelines	<p>ITR マップリゾルバ機能を実行するには、このコマンドを使用してデバイスをイネーブルにします。</p> <p>マップリゾルバ機能を削除するには、このコマンドの no 形式を使用します。</p> <p>マップリゾルバとして設定されたデバイスは、ITR からのカプセル化された Map-Request メッセージを承認し、それらのメッセージのカプセル化を解除し、次に、要求された EID に対して権限を持つ出力トンネルルータ（ETR）を担当するマップサーバにそのメッセージを転送します。マルチサイト環境では、サイトのボーダーでマップリゾルバのプレフィックスリストに基づいて、中継サイトの MSMR またはサイトの MSMR を照会するかどうかが決まります。</p>				

次に、map request メッセージの送信時に 2.1.1.6 のマップリゾルバを使用するように ITR を設定する例を示します。

```
device(config)#router lisp
device(config-router-lisp)#prefix-list wired
device(config-router-lisp-prefix-list)#2001:193:168:1::/64
device(config-router-lisp-prefix-list)#192.168.0.0/16
device(config-router-lisp-prefix-list)#exit-prefix-list
```

```
device(config-router-lisp)#service ipv4
device(config-router-lisp-serv-ipv4)#encapsulation vxlan
device(config-router-lisp-serv-ipv4)#itr map-resolver 2.1.1.6 prefix-list wired
device(config-router-lisp-serv-ipv4)#
```

locator default-set

locator-set をデフォルトとしてマークするには、**locator default-set** コマンドを router-lisp レベルで使用します。

[no] **locator default-set** *rloc-set-name*

Syntax Description

rloc-set-name デフォルトとして設定する locator-set の名前。

Command Default

なし

Command Modes

LISP (router-lisp)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

locator default-set コマンドを使用してデフォルトとして設定された locator-set は、すべてのサービスとインスタンスに適用されます。

locator-set

locator-set を指定して、locator-set コンフィギュレーション モードを開始するには、**locator-set** コマンドを router-lisp レベルで使用します。

[no] **locator-set** *loc-set-name*

Syntax Description	<i>loc-set-name</i> locator-set の名前。				
Command Default	名前				
Command Modes	LISP (router-lisp)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1c</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。				
Usage Guidelines	locator-set を参照する前に、まずその locator-set を定義します。				

map-cache

スタティックエンドポイント ID (EID) をルーティングロケータ (RLOC) の (EID-to-RLOC) マッピング関係に設定するには、instance-service ipv4 モードまたは instance-service ipv6 モードで **map-cache** コマンドを使用します。

```
[no ]map-cache destination-eid-prefix/prefix-len {ipv4-address { priority priority weight weight }
| ipv6-address | map-request | native-forward}
```

Syntax Description

<i>destination-eid-prefix/prefix-len</i>	宛先 IPv4 または IPv6 の EID プレフィックス/プレフィックス長。 この構文にはスラッシュが必要です。
<i>ipv4-address priority priority weight weight</i>	ループバック インターフェイスの IPv4 アドレス。ロケータアドレスに関連付けられたプライオリティと重みは、同じ EID プレフィックス ブロックに複数の RLOC が定義されている場合、トラフィック ポリシーを定義するために使用されます。 Note プライオリティの低いロケータが優先されます。
<i>ipv6-address</i>	ループバック インターフェイスの IPv6 アドレス。
map-request	LISP 宛先 EID に map-request を送信します。
native-forward	この map-request に一致するパケットをネイティブに転送します。

Command Default

なし

Command Modes

LISP インスタンスサービス (router-lisp-instance-service)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

このコマンドの初回使用時には、スタティック IPv4 または IPv6 EID-to-RLOC マッピング関係および関連するトラフィック ポリシーを指定して入力トンネル ルータ (ITR) を設定します。各エントリには、宛先の EID プレフィックスブロックとそれに関連付けられたロケータ、プライオリティ、および重みが入力されます。EID-prefix/prefix-length 引数の値は、宛先サイトの LISP EID プレフィックス ブロックです。ロケータは、IPv4 または IPv6 EID プレフィックスに到達できるリモートサイトの IPv4 または IPv6 アドレスです。ロケータアドレスに関連付けられたプライオリティと重みは、同じ EID プレフィックス ブロックに複数の RLOC が定義されている場合、トラフィック ポリシーを定義するために使用されます。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#map-cache 1.1.1.1/24 map-request
```

map-cache extranet

設定したすべてのエクストラネットプレフィックスをマップキャッシュにインストールするには、instance-service ipv4 モードまたは instance-service ipv6 モードで **map-cache extranet** コマンドを使用します。

map-cache extranet-registration

Command Default	なし				
Command Modes	LISP インスタンスサービス (router-lisp-instance-service)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1c</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。				

Usage Guidelines VRF 間通信をサポートするには、マップサーバマップリゾルバ (MSMR) で **map-cache extranet** コマンドを使用します。このコマンドは、すべてのファブリックの宛先にマップ要求を生成しません。エクストラネットインスタンスの service ipv4 モードまたは service ipv6 モードでこのコマンドを使用します。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#map-cache extranet-registration
```

prefix-list

名前付き LISP プレフィックスセットを定義し、LISP プレフィックスリスト コンフィギュレーション モードを開始するには、ルータ LISP コンフィギュレーション モードで **prefix-list** コマンドを使用します。プレフィックスリストを削除するには、このコマンドの **no** 形式を使用します。

[no] **prefix-list** *prefix-list-name*

Syntax Description	<p>prefix-list <i>prefix-list-name</i></p> <p>使用するプレフィックスリストを指定し、プレフィックスリスト コンフィギュレーション モードを開始します。</p> <p>プレフィックスリストモードで IPv4 EID プレフィックスまたは IPv6 EID プレフィックスを指定します。</p>
---------------------------	---

Command Default プレフィックスリストは定義されていません。

Command Modes LISP (router-lisp)

Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1c</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。				

Usage Guidelines **prefix-list** コマンドは、IPv4 または IPv6 のプレフィックスリストを設定するために使用します。このコマンドを使用すると、ルータがプレフィックスリストコンフィギュレーションモードになり、IPv4 プレフィックスリストまたは IPv6 プレフィックスリストを定義できます。プレフィックスリスト コンフィギュレーションモードを終了するには、**exit-prefix-list** コマンドを使用します。

```
device(config)#router lisp
device(config-router-lisp)#prefix-list wired
device(config-router-prefix-list)#2001:193:168:1::/64
device(config-router-lisp-prefix-list)#192.168.0.0/16
device(config-router-lisp-prefix-list)#exit-prefix-list
```

route-import database

ルーティング情報ベース（RIB）ルートのインポートを設定し、データベースエントリのローカルエンドポイント識別子（EID）プレフィックスを定義してロケータセットに関連付けるには、インスタンスサービスサブモードで **route-import database** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

```
[no] route-import database
{ bgp | connected | eigrp | isis | maximum-prefix | ospf | ospfv3 | rip | static } { [route-map] locator-set
locator-set-name proxy }
```

Syntax Description		
bgp		ボーダー ゲートウェイ プロトコル。BGP プロトコルを使用して RIB ルートを LISP にインポートします。
connected		接続されたルーティングプロトコル
eigrp		Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）。EIGRP プロトコルを使用して RIB ルートを LISP にインポートします。
isis		ISO IS-IS。IS-IS プロトコルを使用して RIB ルートを LISP にインポートします。
ospf		Open Shortest Path First
ospfv3		Open Shortest Path First バージョン 3
maximum-prefix		RIB から取得するプレフィックスの最大数を設定します。
rip		ルーティング情報プロトコル
static		スタティックルートを定義します。
locator-set <i>locator-set-name</i>		作成されたデータベースマッピングエントリで使用するロケータセットを指定します。
proxy		プロキシデータベース マッピングとして RIB ルートのダイナミックインポートを有効にします。
Command Default		なし
Command Modes		LISP インスタンスサービス（router-lisp-instance-service）
Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

プロキシデータベース マッピングとして RIB ルートのダイナミックインポートを有効にするには、**proxy** オプションを指定して **route-import database** コマンドを使用します。RIB インポートを使用するときは、**route-import map-cache** コマンドを使用して対応する RIB マップキャッシュ インポートも設定する必要があります。これが設定されていないと、RIB ルートが存在することになり、着信サイトトラフィックが LISP の対象チェックにパスしません。

次に、プロキシデータベースとして RIB ルートのダイナミックインポートを設定する例を示します。

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#eid-table default
device(config-router-lisp-inst-serv-ipv4)#database-mapping 193.168.0.0/16 locator-set RLOC
proxy
device(config-router-lisp-inst-serv-ipv4)#route-import map-cache bgp 65002 route-map
map-cache-database
device(config-router-lisp-inst-serv-ipv4)#route-import database bgp 65002 locator-set RLOC
proxy
```

service

service コマンドは、その特定のサービスのすべての **instance-service** のインスタンス化の設定テンプレートを作成します。

[no] service {ipv4 | ipv6 | ethernet}

Syntax Description	<p>service ipv4 IPv4 アドレス ファミリのレイヤ 3 ネットワーク サービスをイネーブルにします。</p> <p>service ipv6 IPv6 アドレス ファミリのレイヤ 3 ネットワーク サービスをイネーブルにします。</p> <p>service ethernet レイヤ 2 ネットワーク サービスをイネーブルにします。</p>				
Command Default	なし				
Command Modes	<p>LISP インスタンス (router-lisp-instance)</p> <p>LISP (router-lisp)</p>				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1c</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。				
Usage Guidelines	<p>service コマンドは、instance-id の下にサービスインスタンスを作成し、インスタンスサービスモードを開始します。 service ipv4 または service ipv6 が設定されている同じインスタンスに service ethernet を設定することはできません。</p> <p>service サブモードを終了するには、このコマンドの no 形式を使用します。</p> <pre> device(config)#router lisp device(config-router-lisp)#instance-id 3 device(config-router-lisp-inst)#service ipv4 device(config-router-lisp-inst-serv-ipv4)# device(config)#router lisp device(config-router-lisp)#instance-id 5 device(config-router-lisp-inst)#service ethernet device(config-router-lisp-inst-serv-ethernet)# </pre>				

show lisp instance-id ipv4 database

デバイスのIPv4アドレスファミリーとデータベースマッピングの動作ステータスを表示するには、特権 EXEC モードで **show lisp instance-id ipv4 database** コマンドを使用します。

show lisp instance-id *instance-id* ipv4 database

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines **show lisp instance-id *id* ipv4 database** コマンドは、サイトに設定されている EID プレフィックスを表示するために使用します。次に、出力例を示します。

```
device#show lisp instance-id 101 ipv4 database
LISP ETR IPv4 Mapping Database for EID-table vrf red (IID 101), LSBs: 0x1
Entries total 1, no-route 0, inactive 0
```

```
172.168.0.0/16, locator-set RLOC, proxy
Locator      Pri/Wgt  Source   State
100.110.110.110  1/100  cfg-intf  site-self, reachable
```

```
device#
```

```
device#show lisp instance-id 101 ipv4
Instance ID:                101
Router-lisp ID:              0
Locator table:               default
EID table:                   vrf red
Ingress Tunnel Router (ITR): disabled
Egress Tunnel Router (ETR):  enabled
Proxy-ITR Router (PITR):    enabled RLOCs: 100.110.110.110
Proxy-ETR Router (PETR):    disabled
NAT-traversal Router (NAT-RTR): disabled
Mobility First-Hop Router:  disabled
Map Server (MS):             enabled
Map Resolver (MR):           enabled
Mr-use-petr:                 enabled
Mr-use-petr locator set name: site2
Delegated Database Tree (DDT): disabled
Site Registration Limit:    0
Map-Request source:         derived from EID destination
ITR Map-Resolver(s):        100.77.77.77
                              100.78.78.78
                              100.110.110.110 prefix-list site2
ETR Map-Server(s):          100.77.77.77 (11:25:01)
                              100.78.78.78 (11:25:01)
xTR-ID:                      0xB843200A-0x4566BFC9-0xDAA75B2D-0x8FBE69B0
site-ID:                      unspecified
ITR local RLOC (last resort): 100.110.110.110
ITR Solicit Map Request (SMR): accept and process
  Max SMRs per map-cache entry: 8 more specifics
  Multiple SMR suppression time: 20 secs
```

show lisp instance-id ipv4 database

```
ETR accept mapping data:          disabled, verify disabled
ETR map-cache TTL:                1d00h
Locator Status Algorithms:
  RLOC-probe algorithm:           disabled
  RLOC-probe on route change:     N/A (periodic probing disabled)
  RLOC-probe on member change:    disabled
  LSE reports:                   process
  IPv4 RLOC minimum mask length:  /0
  IPv6 RLOC minimum mask length:  /0
Map-cache:
  Static mappings configured:     1
  Map-cache size/limit:           1/32768
  Imported route count/limit:     0/5000
  Map-cache activity check period: 60 secs
  Map-cache FIB updates:          established
  Persistent map-cache:           disabled
Database:
  Total database mapping size:     1
  static database size/limit:     1/65535
  dynamic database size/limit:    0/65535
  route-import database size/limit: 0/5000
  import-site-reg database size/limit 0/65535
  proxy database size:            1
  Inactive (deconfig/away) size:  0
Encapsulation type:               vxlan
```

show lisp instance-id ipv6 database

デバイスのIPv6アドレスファミリーとデータベースマッピングの動作ステータスを表示するには、特権 EXEC モードで **show lisp instance-id ipv6 database** コマンドを使用します。

show lisp instance-id *instance-id* ipv6 database

Command Default なし

Command Modes 特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines **show lisp instance-id *id* ipv6 database** コマンドは、サイトに設定されている EID プレフィックスを表示するために使用します。次に、出力例を示します。

```
device#show lisp instance-id 101 ipv6 database
LISP ETR IPv6 Mapping Database, LSBs: 0x1

EID-prefix: 2610:D0:1209::/48
  172.16.156.222, priority: 1, weight: 100, state: up, local

device#
```

show lisp instance-id ipv4 map-cache

ITRのIPv4エンドポイント識別子（EID）とリソースロケータ（RLOC）のキャッシュマッピングを表示するには、特権 EXEC モードで **show lisp instance-id ipv4 map-cache** コマンドを使用します。

show lisp instance-id *instance-id* **ipv4 map-cache** [*destination-EID* | *destination-EID-prefix* | **detail**]

Syntax Description	
<i>destination-EID</i>	（任意）EID-to-RLOC マッピングを表示する IPv4 宛先エンドポイント識別子（EID）を指定します。
<i>destination-EID-prefix</i>	（任意）マッピングを表示する IPv4 宛先 EID プレフィックスを指定します（形式は <i>a.b.c.d/nn</i> ）。
detail	（任意）詳細な EID-to-RLOC キャッシュマッピング情報を表示します。

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines このコマンドは、現在のダイナミックおよびスタティック IPv4 EID-to-RLOC マップキャッシュエントリを表示するために使用されます。IPv4 EID または IPv4 EID プレフィックスが指定されていない場合は、現在のすべてのダイナミックおよびスタティック IPv4 EID-to-RLOC マップキャッシュエントリに関する情報のサマリーが一覧表示されます。IPv4 EID または IPv4 EID プレフィックスが指定されている場合は、キャッシュ内の最長一致検索の情報が一覧表示されます。detail オプションを使用すると、現在のすべてのダイナミックおよびスタティック IPv4 EID-to-RLOC マップキャッシュエントリに関するサマリーよりも詳細な情報が表示されます。

次に、**show lisp instance-id ipv4 map-cache** コマンドの出力例を示します。

```
device# show lisp instance-id 102 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

0.0.0.0/0, uptime: 2d14h, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
128.0.0.0/3, uptime: 00:01:44, expires: 00:13:15, via map-reply, unknown-eid-forward
  PETR      Uptime    State    Pri/Wgt    Encap-IID
  55.55.55.1 13:32:40 up       1/100     103
  55.55.55.2 13:32:40 up       1/100     103
  55.55.55.3 13:32:40 up       1/100     103
  55.55.55.4 13:32:40 up       1/100     103
  55.55.55.5 13:32:40 up       5/100     103
  55.55.55.6 13:32:40 up       6/100     103
  55.55.55.7 13:32:40 up       7/100     103
  55.55.55.8 13:32:40 up       8/100     103
150.150.2.0/23, uptime: 11:47:25, expires: 00:06:30, via map-reply, unknown-eid-forward
  PETR      Uptime    State    Pri/Wgt    Encap-IID
```

```

55.55.55.1 13:32:40 up          1/100    103
55.55.55.2 13:32:40 up          1/100    103
55.55.55.3 13:32:40 up          1/100    103
55.55.55.4 13:32:40 up          1/100    103
55.55.55.5 13:32:40 up          5/100    103
55.55.55.6 13:32:40 up          6/100    103
55.55.55.7 13:32:43 up          7/100    103
55.55.55.8 13:32:43 up          8/100    103
150.150.4.0/22, uptime: 13:32:43, expires: 00:05:19, via map-reply, unknown-eid-forward
  PETR      Uptime    State     Pri/Wgt   Encap-IID
55.55.55.1 13:32:43 up        1/100    103
55.55.55.2 13:32:43 up        1/100    103
55.55.55.3 13:32:43 up        1/100    103
55.55.55.4 13:32:43 up        1/100    103
55.55.55.5 13:32:43 up        5/100    103
55.55.55.6 13:32:43 up        6/100    103
55.55.55.7 13:32:43 up        7/100    103
55.55.55.8 13:32:43 up        8/100    103
150.150.8.0/21, uptime: 13:32:35, expires: 00:05:27, via map-reply, unknown-eid-forward
  PETR      Uptime    State     Pri/Wgt   Encap-IID
55.55.55.1 13:32:43 up        1/100    103
55.55.55.2 13:32:43 up        1/100    103
55.55.55.3 13:32:43 up        1/100    103
55.55.55.4 13:32:43 up        1/100    103
55.55.55.5 13:32:43 up        5/100    103
55.55.55.6 13:32:43 up        6/100    103
55.55.55.7 13:32:43 up        7/100    103
55.55.55.8 13:32:45 up        8/100    103
171.171.0.0/16, uptime: 2d14h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
172.172.0.0/16, uptime: 2d14h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
178.168.2.1/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator   Uptime    State     Pri/Wgt   Encap-IID
11.11.11.1 2d14h    up        1/100    -
178.168.2.2/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator   Uptime    State     Pri/Wgt   Encap-IID
11.11.11.1 2d14h    up        1/100    -
178.168.2.3/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator   Uptime    State     Pri/Wgt   Encap-IID
11.11.11.1 2d14h    up        1/100    -
178.168.2.4/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator   Uptime    State     Pri/Wgt   Encap-IID
11.11.11.1 2d14h    up        1/100    -
178.168.2.5/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator   Uptime    State     Pri/Wgt   Encap-IID
11.11.11.1 2d14h    up        1/100    -
178.168.2.6/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator   Uptime    State     Pri/Wgt   Encap-IID

```

device#show lisp instance-id 102 ipv4 map-cache detail

LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

```

0.0.0.0/0, uptime: 2d15h, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 2d15h, map-source: local
  Exempt, Packets out: 30531(17585856 bytes) (~ 00:01:36 ago)
  Configured as EID address space
  Negative cache entry, action: send-map-request
128.0.0.0/3, uptime: 00:02:02, expires: 00:12:57, via map-reply, unknown-eid-forward
  Sources: map-reply
  State: unknown-eid-forward, last modified: 00:02:02, map-source: local
  Active, Packets out: 9(5184 bytes) (~ 00:00:36 ago)
  PETR      Uptime    State     Pri/Wgt   Encap-IID
55.55.55.1 13:32:58 up        1/100    103

```

show lisp instance-id ipv4 map-cache

```

55.55.55.2 13:32:58 up          1/100    103
55.55.55.3 13:32:58 up          1/100    103
55.55.55.4 13:32:58 up          1/100    103
55.55.55.5 13:32:58 up          5/100    103
55.55.55.6 13:32:58 up          6/100    103
55.55.55.7 13:32:58 up          7/100    103
55.55.55.8 13:32:58 up          8/100    103
150.150.2.0/23, uptime: 11:47:43, expires: 00:06:12, via map-reply, unknown-eid-forward
Sources: map-reply
State: unknown-eid-forward, last modified: 11:47:44, map-source: local
Active, Packets out: 4243(2443968 bytes) (~ 00:00:38 ago)
PETR      Uptime    State     Pri/Wgt   Encap-IID
55.55.55.1 13:33:00 up        1/100     103
55.55.55.2 13:33:00 up        1/100     103
55.55.55.3 13:33:00 up        1/100     103
55.55.55.4 13:33:00 up        1/100     103
55.55.55.5 13:33:00 up        5/100     103
55.55.55.6 13:33:00 up        6/100     103
55.55.55.7 13:33:00 up        7/100     103
55.55.55.8 13:33:00 up        8/100     103
150.150.4.0/22, uptime: 13:33:00, expires: 00:05:02, via map-reply, unknown-eid-forward
Sources: map-reply
State: unknown-eid-forward, last modified: 13:33:00, map-source: local
Active, Packets out: 4874(2807424 bytes) (~ 00:00:38 ago)
PETR      Uptime    State     Pri/Wgt   Encap-IID
55.55.55.1 13:33:00 up        1/100     103
55.55.55.2 13:33:00 up        1/100     103
55.55.55.3 13:33:00 up        1/100     103
55.55.55.4 13:33:00 up        1/100     103
55.55.55.5 13:33:00 up        5/100     103
55.55.55.6 13:33:00 up        6/100     103
55.55.55.7 13:33:01 up        7/100     103
55.55.55.8 13:33:01 up        8/100     103
150.150.8.0/21, uptime: 13:32:53, expires: 00:05:09, via map-reply, unknown-eid-forward
Sources: map-reply
State: unknown-eid-forward, last modified: 13:32:53, map-source: local
Active, Packets out: 4874(2807424 bytes) (~ 00:00:39 ago)
PETR      Uptime    State     Pri/Wgt   Encap-IID
55.55.55.1 13:33:01 up        1/100     103
55.55.55.2 13:33:01 up        1/100     103
55.55.55.3 13:33:01 up        1/100     103
55.55.55.4 13:33:01 up        1/100     103
55.55.55.5 13:33:01 up        5/100     103
55.55.55.6 13:33:01 up        6/100     103
55.55.55.7 13:33:01 up        7/100     103
55.55.55.8 13:33:01 up        8/100     103
171.171.0.0/16, uptime: 2d15h, expires: never, via dynamic-EID, send-map-request
Sources: NONE
State: send-map-request, last modified: 2d15h, map-source: local
Exempt, Packets out: 2(1152 bytes) (~ 2d14h ago)
Configured as EID address space
Configured as dynamic-EID address space
Encapsulating dynamic-EID traffic
Negative cache entry, action: send-map-request
172.172.0.0/16, uptime: 2d15h, expires: never, via dynamic-EID, send-map-request
Sources: NONE
State: send-map-request, last modified: 2d15h, map-source: local
Exempt, Packets out: 2(1152 bytes) (~ 2d14h ago)
Configured as EID address space
Configured as dynamic-EID address space
Encapsulating dynamic-EID traffic
Negative cache entry, action: send-map-request
178.168.2.1/32, uptime: 2d14h, expires: 09:26:55, via map-reply, complete
Sources: map-reply

```

```

State: complete, last modified: 2d14h, map-source: 48.1.1.4
Active, Packets out: 22513(12967488 bytes) (~ 00:00:41 ago)
Locator    Uptime    State    Pri/Wgt    Encap-IID
11.11.11.1 2d14h    up       1/100      -
  Last up-down state change:      2d14h, state change count: 1
  Last route reachability change:  2d14h, state change count: 1
  Last priority / weight change:   never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent:          2d14h (rtt 92ms)
178.168.2.2/32, uptime: 2d14h, expires: 09:26:55, via map-reply, complete
Sources: map-reply
State: complete, last modified: 2d14h, map-source: 48.1.1.4
Active, Packets out: 22513(12967488 bytes) (~ 00:00:45 ago)
Locator    Uptime    State    Pri/Wgt    Encap-IID
11.11.11.1 2d14h    up       1/100      -
  Last up-down state change:      2d14h, state change count: 1
  Last route reachability change:  2d14h, state change count: 1
  Last priority / weight change:   never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent:          2d14h (rtt 91ms)
178.168.2.3/32, uptime: 2d14h, expires: 09:26:51, via map-reply, complete
Sources: map-reply
State: complete, last modified: 2d14h, map-source: 48.1.1.4
Active, Packets out: 22513(12967488 bytes) (~ 00:00:45 ago)
Locator    Uptime    State    Pri/Wgt    Encap-IID
11.11.11.1 2d14h    up       1/100      -
  Last up-down state change:      2d14h, state change count: 1
  Last route reachability change:  2d14h, state change count: 1
  Last priority / weight change:   never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent:          2d14h (rtt 91ms)
178.168.2.4/32, uptime: 2d14h, expires: 09:26:51, via map-reply, complete
Sources: map-reply
State: complete, last modified: 2d14h, map-source: 48.1.1.4

device#show lisp instance-id 102 ipv4 map-cache 178.168.2.3/32
LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

178.168.2.3/32, uptime: 2d14h, expires: 09:26:25, via map-reply, complete
Sources: map-reply
State: complete, last modified: 2d14h, map-source: 48.1.1.4
Active, Packets out: 22519(12970944 bytes) (~ 00:00:11 ago)
Locator    Uptime    State    Pri/Wgt    Encap-IID
11.11.11.1 2d14h    up       1/100      -
  Last up-down state change:      2d14h, state change count: 1
  Last route reachability change:  2d14h, state change count: 1
  Last priority / weight change:   never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent:          2d14h (rtt 91ms)

device#show lisp instance-id 102 ipv4 map-cache 178.168.2.3
LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

178.168.2.3/32, uptime: 2d14h, expires: 09:26:14, via map-reply, complete
Sources: map-reply
State: complete, last modified: 2d14h, map-source: 48.1.1.4
Active, Packets out: 22519(12970944 bytes) (~ 00:00:22 ago)
Locator    Uptime    State    Pri/Wgt    Encap-IID
11.11.11.1 2d14h    up       1/100      -
  Last up-down state change:      2d14h, state change count: 1
  Last route reachability change:  2d14h, state change count: 1
  Last priority / weight change:   never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent:          2d14h (rtt 91ms)
OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 sta

```

show lisp instance-id ipv4 map-cache

```

OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 stat
OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 ipv4 stat
OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 ipv4 statistics
LISP EID Statistics for instance ID 102 - last cleared: never
Control Packets:
  Map-Requests in/out:                               5911/66032
    Map-Request receive rate (5 sec/1 min/5 min):    0.00/ 0.00/ 0.00
    Encapsulated Map-Requests in/out:                0/60600
    RLOC-probe Map-Requests in/out:                  5911/5432
    SMR-based Map-Requests in/out:                   0/0
    Extranet SMR cross-IID Map-Requests in:          0
    Map-Requests expired on-queue/no-reply           0/0
    Map-Resolver Map-Requests forwarded:             0
    Map-Server Map-Requests forwarded:               0
  Map-Reply records in/out:                           64815/5911
    Authoritative records in/out:                    12696/5911
    Non-authoritative records in/out:                 52119/0
    Negative records in/out:                          8000/0
    RLOC-probe records in/out:                       4696/5911
    Map-Server Proxy-Reply records out:               0
  WLC Map-Subscribe records in/out:                   0/4
    Map-Subscribe failures in/out:                   0/0
  WLC Map-Unsubscribe records in/out:                 0/0
    Map-Unsubscribe failures in/out:                 0/0
  Map-Register records in/out:                       0/8310
    Map-Register receive rate (5 sec/1 min/5 min):    0.00/ 0.00/ 0.00
    Map-Server AF disabled:                           0
    Authentication failures:                          0
  WLC Map-Register records in/out:                   0/0
    WLC AP Map-Register in/out:                      0/0
    WLC Client Map-Register in/out:                  0/0
    WLC Map-Register failures in/out:                 0/0
  Map-Notify records in/out:                         20554/0
    Authentication failures:                           0
  WLC Map-Notify records in/out:                     0/0
    WLC AP Map-Notify in/out:                         0/0
    WLC Client Map-Notify in/out:                    0/0
    WLC Map-Notify failures in/out:                   0/0
  Publish-Subscribe in/out:
    Subscription Request records in/out:              0/6
    Subscription Request failures in/out:              0/0
    Subscription Status records in/out:                4/0
      End of Publication records in/out:               4/0
      Subscription rejected records in/out:            0/0
      Subscription removed records in/out:             0/0
    Subscription Status failures in/out:              0/0
    Solicit Subscription records in/out:               0/0
    Solicit Subscription failures in/out:              0/0
    Publication records in/out:                       0/0
    Publication failures in/out:                      0/0
Errors:
  Mapping record TTL alerts:                           0
  Map-Request invalid source rloc drops:              0
  Map-Register invalid source rloc drops:             0
  DDT Requests failed:                                0
  DDT ITR Map-Requests dropped:                       0 (nonce-collision: 0, bad-xTR-nonce:
0)
Cache Related:
  Cache entries created/deleted:                      200103/196095
  NSF CEF replay entry count                           0
  Number of EID-prefixes in map-cache:                4008
  Number of rejected EID-prefixes due to limit :      0
  Number of negative entries in map-cache:             8
  Total number of RLOCs in map-cache:                 4000

```

```

Average RLOCs per EID-prefix:                1
Forwarding:
  Number of data signals processed:            199173 (+ dropped 5474)
  Number of reachability reports:             0 (+ dropped 0)
  Number of SMR signals dropped:              0
ITR Map-Resolvers:
  Map-Resolver      LastReply  Metric ReqsSent  Positive Negative No-Reply  AvgRTT(5
sec/1 min/5 min)
  44.44.44.44       00:03:11      6      62253      19675      8000      0      0.00/
0.00/10.00
  66.66.66.66       never         Unreach      0          0          0          0      0.00/ 0.00/
0.00
ETR Map-Servers:
  Map-Server      AvgRTT(5 sec/1 min/5 min)
  44.44.44.44     0.00/ 0.00/ 0.00
  66.66.66.66     0.00/ 0.00/ 0.00
LISP RLOC Statistics - last cleared: never
Control Packets:
  RTR Map-Requests forwarded:                0
  RTR Map-Notifies forwarded:                0
  DDT-Map-Requests in/out:                   0/0
  DDT-Map-Referrals in/out:                   0/0
Errors:
  Map-Request format errors:                  0
  Map-Reply format errors:                    0
  Map-Referral format errors:                 0
LISP Miscellaneous Statistics - last cleared: never
Errors:
  Invalid IP version drops:                   0
  Invalid IP header drops:                    0
  Invalid IP proto field drops:               0
  Invalid packet size drops:                  0
  Invalid LISP control port drops:            0
  Invalid LISP checksum drops:                0
  Unsupported LISP packet type drops:         0
  Unknown packet drops:                       0

```

show lisp instance-id ipv6 map-cache

ITRのリソースロケータ（RLOC）のキャッシュマッピングへのIPv6エンドポイント識別子（EID）を表示するには、特権 EXEC モードで **show lisp instance-id ipv6 map-cache** コマンドを使用します。

show lisp instance-id *instance-id* **ipv6 map-cache** [*destination-EID* | *destination-EID-prefix* | **detail**]

Syntax Description	
<i>destination-EID</i>	（任意）EID-to-RLOC マッピングを表示する IPv4 宛先エンドポイント識別子（EID）を指定します。
<i>destination-EID-prefix</i>	（任意）マッピングを表示する IPv4 宛先 EID プレフィックスを指定します（形式は <i>a.b.c.d/nn</i> ）。
detail	（任意）詳細な EID-to-RLOC キャッシュマッピング情報を表示します。

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines このコマンドは、現在のダイナミックおよびスタティック IPv6 EID-to-RLOC マップキャッシュエントリを表示するために使用されます。IPv6 EID または IPv6 EID プレフィックスが指定されていない場合は、現在のすべてのダイナミックおよびスタティック IPv4 EID-to-RLOC マップキャッシュエントリに関する情報のサマリーが一覧表示されます。IPv6 EID または IPv6 EID プレフィックスが指定されている場合は、キャッシュ内の最長一致検索の情報が一覧表示されます。detail オプションを使用すると、現在のすべてのダイナミックおよびスタティック IPv6 EID-to-RLOC マップキャッシュエントリに関するサマリーよりも詳細な情報が表示されます。

次に、**show lisp instance-id ipv6 map-cache** コマンドの出力例を示します。

```
device# show lisp instance-id 101 ipv6 map-cache
LISP IPv6 Mapping Cache, 2 entries

::/0, uptime: 00:00:26, expires: never, via static
  Negative cache entry, action: send-map-request
2001:DB8:AB::/48, uptime: 00:00:04, expires: 23:59:53, via map-reply, complete
  Locator    Uptime    State    Pri/Wgt
  10.0.0.6   00:00:04  up      1/100
```

次に、現在のダイナミックおよびスタティック IPv6 EID-to-RLOC マップキャッシュエントリの詳細なリストを表示する **show lisp instance-id x ipv6 map-cache detail** コマンドの出力例を示します。

```
device#show lisp instance-id 101 ipv6 map-cache detail
LISP IPv6 Mapping Cache, 2 entries

::/0, uptime: 00:00:52, expires: never, via static
```

```

State: send-map-request, last modified: 00:00:52, map-source: local
Idle, Packets out: 0
Negative cache entry, action: send-map-request
2001:DB8:AB::/48, uptime: 00:00:30, expires: 23:59:27, via map-reply, complete
State: complete, last modified: 00:00:30, map-source: 10.0.0.6
Active, Packets out: 0
Locator  Uptime    State    Pri/Wgt
10.0.0.6  00:00:30  up      1/100
  Last up-down state change:      never, state change count: 0
  Last priority / weight change:  never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent:         never

```

特定の IPv6 EID プレフィックスを使用した `show ipv6 lisp map-cache` コマンドの次の出力例は、その IPv6 EID プレフィックスエントリに関連付けられた詳細情報を表示します。

```

device#show lisp instance-id 101 ipv6 map-cache 2001:DB8:AB::/48
LISP IPv6 Mapping Cache, 2 entries

2001:DB8:AB::/48, uptime: 00:01:02, expires: 23:58:54, via map-reply, complete
State: complete, last modified: 00:01:02, map-source: 10.0.0.6
Active, Packets out: 0
Locator  Uptime    State    Pri/Wgt
10.0.0.6  00:01:02  up      1/100
  Last up-down state change:      never, state change count: 0
  Last priority / weight change:  never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent:         never

```

show lisp instance-id ipv4 server

LISP サイト登録情報を表示するには、特権 EXEC モードで **show lisp instance-id ipv4 server** コマンドを使用します。

show lisp instance-id *instance-id***ipv4 server** [*EID-address* | *EID-prefix* | **detail** | **name** | **rloc** | **summary**]

Syntax Description	
<i>EID-address</i>	(任意) このエンドポイントのサイト登録情報を表示します。
<i>EID-prefix</i>	(任意) この IPv4 EID プレフィックスのサイト登録情報を表示します。
detail	(任意) 詳細なサイト情報を表示します。
name	(任意) 指定したサイトのサイト登録情報を表示します。
rloc	(任意) RLOC-EID インスタンスメンバーシップの詳細を表示します。
summary	(任意) 各サイトのサマリー情報を表示します。

Command Default なし

Command Modes 特権 EXEC

Command History

リリー	変更内容
ス	
このコマンドが導入されました。	

Usage Guidelines トンネルルータ (xTR) によってホストが検出されると、マップサーバ (MS) に登録されます。サイト登録の詳細を表示するには、**show lisp instance-id x ipv4 server** コマンドを使用します。TCP 登録についてはポート番号が表示されますが、UDP 登録についてはポート番号は表示されません。UDP 登録のデフォルトのポート番号は 4342 です。

次に、このコマンドの出力例を示します。

```
device# show lisp instance-id 100 ipv4 server
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up      Who Last      Inst      EID Prefix
                Register  Up      Registered  ID
XTR            00:03:22 yes*#   172.16.1.4:64200  100      101.1.0.0/16
                00:03:16 yes#    172.16.1.3:19881  100      101.1.1.1/32

device# show lisp instance-id 100 ipv4 server 101.1.0.0/16
LISP Site Registration Information

Site name: XTR
Allowed configured locators: any
Requested EID-prefix:
```

```

EID-prefix: 101.1.0.0/16 instance-id 100
First registered: 00:04:24
Last registered: 00:04:20
Routing table tag: 0
Origin: Configuration, accepting more specifics
Merge active: No
Proxy reply: No
TTL: 1d00h
State: complete
Registration errors:
  Authentication failures: 0
  Allowed locators mismatch: 0
ETR 172.16.1.4:64200, last registered 00:04:20, no proxy-reply, map-notify
  TTL 1d00h, no merge, hash-function sha1, nonce 0xC1ED8EE1-0x553D05D4

state complete, no security-capability
xTR-ID 0x46B2F3A5-0x19B0A3C5-0x67055A44-0xF5BF3FBB
site-ID unspecified
sourced by reliable transport
Locator      Local  State      Pri/Wgt  Scope
172.16.1.4  yes   admin-down 255/100  IPv4 none

```

次に、UDP 登録についての出力（ポート番号なし）を示します。

```

device# show lisp instance-id 100 ipv4 server 101.1.1.1/32
LISP Site Registration Information

Site name: XTR
Allowed configured locators: any
Requested EID-prefix:

EID-prefix: 101.1.1.1/32 instance-id 100
First registered: 00:00:08
Last registered: 00:00:04
Routing table tag: 0
Origin: Dynamic, more specific of 101.1.0.0/16
Merge active: No
Proxy reply: No
TTL: 1d00h
State: complete
Registration errors:
  Authentication failures: 0
  Allowed locators mismatch: 0
ETR 172.16.1.3:46245, last registered 00:00:04, no proxy-reply, map-notify
  TTL 1d00h, no merge, hash-function sha1, nonce 0x1769BD91-0x06E10A06

state complete, no security-capability
xTR-ID 0x4F5F0056-0xAE270416-0x360B42D6-0x6FCD3F5B
site-ID unspecified
sourced by reliable transport
Locator      Local  State      Pri/Wgt  Scope
172.16.1.3  yes   up         100/100  IPv4 none
ETR 172.16.1.3, last registered 00:00:08, no proxy-reply, map-notify
  TTL 1d00h, no merge, hash-function sha1, nonce 0x1769BD91-0x06E10A06
state complete, no security-capability
xTR-ID 0x4F5F0056-0xAE270416-0x360B42D6-0x6FCD3F5B
site-ID unspecified
Locator      Local  State      Pri/Wgt  Scope
172.16.1.3  yes   up         100/100  IPv4 none

```

show lisp instance-id ipv6 server

LISP サイト登録情報を表示するには、特権 EXEC モードで **show lisp instance-id ipv6 server** コマンドを使用します。

show lisp instance-id *instance-id* ipv6 server [*EID-address* | *EID-prefix* | **detail** | **name** | **rloc** | **summary**]

Syntax Description	
<i>EID-address</i>	(任意) このエンドポイントのサイト登録情報を表示します。
<i>EID-prefix</i>	(任意) この IPv6 EID プレフィックスのサイト登録情報を表示します。
detail	(任意) 詳細なサイト情報を表示します。
name	(任意) 指定したサイトのサイト登録情報を表示します。
rloc	(任意) RLOC-EID インスタンスメンバーシップの詳細を表示します。
summary	(任意) 各サイトのサマリー情報を表示します。

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines トンネルルータ (xTR) によってホストが検出されると、マップサーバ (MS) に登録されます。サイト登録の詳細を表示するには、**show lisp instance-id ipv6 server** コマンドを使用します。

show lisp instance-id ipv4 statistics

Locator/ID Separation Protocol (LISP) IPv4 アドレスファミリーパケット数の統計情報を表示するには、特権 EXEC モードで **show lisp instance-id ipv4 statistics** コマンドを使用します。

show lisp instance-id *instance-id* ipv4 statistics

Command Default

なし

Command Modes

特権 EXEC

Command History

リリース	変更内容
------	------

Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。
---------------------------------	-----------------

Usage Guidelines

このコマンドは、パケットのカプセル化、カプセル化解除、Map-Request、Map-Reply、Map-Register、およびその他の LISP 関連のパケットに関連した IPv4 LISP 統計情報を表示するために使用します。

次に、このコマンドの出力例を示します。

```
device# show lisp instance-id 100 ipv4 statistics
```

show lisp instance-id ipv6 statistics

Locator/ID Separation Protocol (LISP) IPv6 アドレスファミリーパケット数の統計情報を表示するには、特権 EXEC モードで **show lisp instance-id ipv6 statistics** コマンドを使用します。

show lisp instance-id *instance-id* ipv6 statistics

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines このコマンドは、パケットのカプセル化、カプセル化解除、Map-Request、Map-Reply、Map-Register、およびその他の LISP 関連のパケットに関連した IPv4 LISP 統計情報を表示するために使用します。

次に、このコマンドの出力例を示します。

```
device# show lisp instance-id 100 ipv6 statistics
```

show lisp prefix-list

LISP プレフィックスリスト情報を表示するには、特権 EXEC モードで **show lisp prefix-list** コマンドを使用します。

show lisp prefix-list [*name-prefix-list*]

Syntax Description	<i>name-prefix-list</i> (任意) 情報を表示するプレフィックスリストを指定します。
---------------------------	---

Command Default	なし
------------------------	----

Command Modes	特権 EXEC
----------------------	---------

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines	次に、 show lisp prefix-list コマンドの出力例を示します。
-------------------------	---

```
device# show lisp prefix-list
Lisp Prefix List information for router lisp 0

Prefix List: set
  Number of entries: 1
  Entries:
  1.2.3.4/16
  Sources: static
```

show lisp session

ファブリック内の信頼性の高いトランスポートセッションの現在のリストを表示するには、特権 EXEC モードで **show lisp session** コマンドを使用します。

show lisp session [**all** | **established**]

Syntax Description	all (任意) すべてのセッションのトランスポートセッション情報を表示します。
	established (任意) 確立された接続のトランスポートセッション情報を表示します。
Command Default	なし
Command Modes	特権 EXEC
Command History	リリース 変更内容 Cisco IOS XE Gibraltar 16.11.1c このコマンドが導入されました。

Usage Guidelines **show lisp session** コマンドでは、アップ状態またはダウン状態のセッションのみが表示されます。状態に関係なくすべてのセッションを表示するには、**show lisp session all** コマンドを使用します。

次に、MSMR での **show lisp session** コマンドの出力例を示します。

```
device# show lisp session
Sessions for VRF default, total: 4, established: 2
Peer                State      Up/Down      In/Out      Users
172.16.1.3:22667    Up         00:00:52     4/8         2
172.16.1.4:18904    Up         00:22:15     5/13        1

device# show lisp session all
Sessions for VRF default, total: 4, established: 2
Peer                State      Up/Down      In/Out      Users
172.16.1.3          Listening   never         0/0         0
172.16.1.3:22667    Up         00:01:13     4/8         2
172.16.1.4          Listening   never         0/0         0
172.16.1.4:18904    Up         00:22:36     5/13        1
```

use-petr

ルータを設定して IPv4 または IPv6 Locator/ID Separation Protocol (LISP) プロキシ出力トンネルルータ (PETR) を使用するには、LISP インスタンス コンフィギュレーションモードまたは LISP インスタンス サービス コンフィギュレーション モードで **use-petr** コマンドを使用します。LISP PETR の使用を止めるには、このコマンドの **no** 形式を使用します。

[no] **use-petr** *locator-address* [**priority** *priority* **weight** *weight*]

Syntax Description	
<i>locator-address</i>	デフォルトとして設定する locator-set の名前。
priority <i>priority</i>	(任意) この PETR に割り当てるプライオリティ (0 ~ 255 の値) を指定します。値が小さいほど、プライオリティは高くなります。
weight <i>weight</i>	(任意) 負荷分散するトラフィックのパーセンテージ (0 ~ 100 の値) を指定します。

Command Default ルータは PETR サービスを使用しません。

Command Modes LISP サービス (router-lisp-service)
LISP インスタンスサービス (router-lisp-instance-service)

Command History

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1c	このコマンドが導入されました。

Usage Guidelines

IPv4 プロキシ出力トンネルルータ (PETR) サービスを使用するには、**use-petr** コマンドを使用して入力トンネルルータ (ITR) またはプロキシ入力トンネルルータ (PITR) を有効にします。PETR サービスの使用がイネーブルになっている場合は、LISP 以外のサイトに宛てた LISP エンドポイント ID (EID) (ソース) パケットをネイティブに転送するのではなく、これらのパケットが LISP でカプセル化され、PETR に転送されます。これらのパケットを受信すると、PETR はそれらのパケット化を解除して、LISP 以外の宛先にネイティブに転送します。

サービスイーサネット コンフィギュレーション モードでは、**use-petr** コマンドを使用しないでください。

PETR サービスは、複数のケースで必要な場合があります。

1. デフォルトでは、LISP サイトが LISP 以外のサイトにネイティブにパケットを転送する場合 (LISP カプセル化されていない)、パケットの送信元 IP アドレスは、EID のアドレスです。アクセスネットワークのプロバイダー側がストリクトユニキャストリバースパス転送 (uRPF) またはアンチスプーフィングアクセスリストで設定されている場合、これらのパケットはスプーフィングしてドロップするものと見なされます。これは、EID がプロバイダーのコアネットワークでアドバタイズされないためです。この場合、LISP 以外のサイトにネイティブにパ

ケットを転送する代わりに、ITR は、送信元アドレスとしてサイト ロケータ、宛先アドレスとして PETR を使用して、これらのパケットをカプセル化します。



Note **use-petr** コマンドを使用しても LISP から LISP へ、または LISP 以外から LISP 以外への転送動作は変更されません。LISP サイト宛の LISP EID パケットは通常の LISP 転送プロセスに従い、通常どおり宛先 ETR に直接送信されます。LISP 以外から LISP 以外へのパケットは、LISP カプセル化の候補となることはなく、常に通常のプロセスに従ってネイティブに転送されます。

2. LISP IPv6 (EID) サイトが LISP 以外の IPv6 サイトに接続する必要があり、ITR ロケータまたは中間ネットワークの一部が IPv6 をサポートしない (IPv4 専用) 場合は、PETR に IPv4 と IPv6 の両方の接続性があると想定し、PETR を使用してアドレス ファミリの非互換性を通過 (ホップ オーバー) することができます。この場合、ITR は PETR 宛の IPv4 ロケータで IPv6 の EID を LISP によりカプセル化でき、PETR がそのパケットのカプセル化を解除して、それらを IPv6 接続を経由して LISP 以外の IPv6 サイトにネイティブに転送します。この場合、PETR を効果的に使用することで、LISP サイトのパケットは、LISP 混在プロトコルのカプセル化サポートを使用してネットワークの IPv4 部分を通過することができます。

Examples

次に、IPv4 ロケータ 10.1.1.1 で PETR を使用するように ITR を設定する例を示します。この場合、LISP 以外の IPv4 サイトに宛てた LISP サイトの IPv4 EID が 10.1.1.1 にある PETR 宛の IPv4 LISP ヘッダー内にカプセル化されます。

```
device(config)# router lisp
device(config-router-lisp) #service ipv4
device(config-router-lisp-serv-ipv4) # use-petr 10.1.1.1
```

次に、2つの PETR を使用するように ITR を設定する例を示します。これらの PETR のうちの1つは IPv4 ロケータが 10.1.1.1 でプライマリ PETR (プライオリティ 1、重み 100) として設定され、もう1つには IPv4 ロケータが 10.1.2.1 でセカンダリ PETR (プライオリティ 2、重み 100) として設定されています。この場合、LISP 以外の IPv4 サイトに宛てた LISP サイトの IPv4 EID は、失敗しない限り、10.1.1.1 にあるプライマリ PETR への IPv4 LISP ヘッダー内にカプセル化されます。失敗した場合は、セカンダリが使用されます。

```
Router(config-router-lisp-serv-ipv4) # use-petr 10.1.1.1 priority 1 weight 100
Router(config-router-lisp-serv-ipv4) # use-petr 10.1.2.1 priority 2 weight 100
```



PART II

Cisco TrustSec

- [Cisco TrustSec コマンド](#), on page 71



Cisco TrustSec コマンド

- [address \(CTS\)](#) , on page 73
- [clear cts environment-data](#), on page 75
- [clear cts policy-server statistics](#), on page 76
- [content-type json](#), on page 77
- [cts authorization list](#), on page 78
- [cts change-password](#), on page 80
- [cts credentials](#), on page 81
- [cts environment-data enable](#), on page 83
- [cts policy-server device-id](#), on page 84
- [cts policy-server name](#), on page 85
- [cts policy-server order random](#), on page 86
- [cts policy-server username](#), on page 87
- [cts refresh](#), on page 89
- [cts rekey](#), on page 91
- [cts role-based enforcement](#), on page 92
- [cts role-based l2-vrf](#), on page 94
- [cts role-based monitor](#), on page 96
- [cts role-based permissions](#), on page 98
- [cts role-based sgt-caching](#), on page 100
- [cts role-based sgt-map](#), on page 101
- [cts sxp connection peer](#), on page 104
- [cts sxp default password](#), on page 107
- [cts sxp default source-ip](#), on page 109
- [cts sxp filter-enable](#), on page 111
- [cts sxp filter-group](#), on page 112
- [cts sxp filter-list](#), on page 114
- [cts sxp log binding-changes](#), on page 116
- [cts sxp reconciliation period](#), on page 117
- [cts sxp retry period](#), on page 118
- [debug cts environment-data](#), on page 119
- [debug cts policy-server](#), on page 121
- [port \(CTS\)](#) , on page 122
- [propagate sgt \(cts manual\)](#), on page 123

- retransmit (CTS) , on page 125
- sap mode-list (cts manual), on page 126
- show cts credentials, on page 128
- show cts environment-data, on page 129
- show cts interface, on page 130
- show cts policy-server, on page 133
- show cts role-based counters, on page 136
- show cts role-based permissions, on page 138
- show cts server-list, on page 140
- show cts sxp, on page 143
- show platform hardware fed switch active fwd-asic resource team utilization , on page 146
- show platform hardware fed switch active sgacl resource usage, on page 148
- show platform software classification switch active F0 class-group-manager class-group client acl all, on page 149
- show platform software cts forwarding-manager switch active F0 port, on page 150
- show platform software cts forwarding-manager switch active F0, on page 154
- show platform software cts forwarding-manager switch active F0 permissions, on page 155
- show platform software fed switch active acl counters hardware | inc SGACL , on page 157
- show platform software fed switch active acl usage , on page 158
- show platform software fed switch active ifm mappings , on page 159
- show platform software fed switch active ip route , on page 162
- show platform software fed switch active sgacl detail , on page 164
- show platform software fed switch active sgacl port , on page 165
- show platform software fed switch active sgacl vlan , on page 167
- show platform software status control-processor brief, on page 168
- show monitor capture <name> buffer, on page 169
- timeout (CTS) , on page 170
- tls server-trustpoint, on page 171

address (CTS)

Cisco TrustSec ポリシーサーバのアドレスを設定するには、ポリシーサーバコンフィギュレーションモードで **address** コマンドを使用します。ポリシーサーバのアドレスを削除するには、このコマンドの **no** 形式を使用します。

address {*domain-name name* | **ipv4** *policy-server-address* | **ipv6** *policy-server-address*}
no address {*domain-name* | **ipv4** | **ipv6**}

Syntax Description	domain-name <i>name</i>	ポリシーサーバのドメイン名を指定します。
	ipv4 <i>policy-server-address</i>	ポリシーサーバの IP アドレスを指定します。
	ipv6	ポリシーサーバの IPv6 アドレスを指定します。
Command Default	ポリシーサーバのアドレスは設定されていません。	
Command Modes	ポリシーサーバ コンフィギュレーション (config-policy-server)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines ポリシーサーバ コンフィギュレーションモードを開始するには、ポリシーサーバ名を設定します。

Examples

次に、ポリシーサーバのドメイン名を設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# address domain-name ISE_domain
```

次に、ポリシーサーバの IP アドレスを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server name ise_server_2
Device(config-policy-server)# address ipv4 10.1.1.1
```

Related Commands

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。

clear cts environment-data

Cisco TrustSec の環境データをクリアするには、特権 EXEC モードで **clear cts environment-data** コマンドを使用します。

clear cts environment-data

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、環境データをクリアする例を示します。

```
Device# enable
Device# clear cts environment-data
```

Related Commands

コマンド	説明
cts environment-data enable	環境データのダウンロードを有効にします。
debug cts environment-data	Cisco TrustSec 環境データ操作のデバッグを有効にします。
show cts environment-data	Cisco TrustSec の環境データ情報を表示します。

clear cts policy-server statistics

Cisco TrustSec ポリシーサーバの統計情報をクリアするには、特権 EXEC モードで **clear cts policy-server statistics** コマンドを使用します。

clear cts policy-server statistics {**active** | **all**}

Syntax Description	active	アクティブなすべてのポリシーサーバの統計情報をクリアします。
	all	すべてのポリシーサーバの統計情報をクリアします。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、すべてのポリシーサーバの統計情報をクリアする例を示します。

```
Device# enable
Device# clear cts policy-server statistics all
```

Related Commands	コマンド	説明
	cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバコンフィギュレーションモードを開始します。

content-type json

JavaScript Object Notation (JSON) をコンテンツタイプとして有効にするには、ポリシーサーバコンフィギュレーション モードで **content-type json** コマンドを使用します。このコンテンツタイプを削除するには、このコマンドの **no** 形式を使用します。

content-type json
no content-type json

このコマンドには引数またはキーワードはありません。

Command Default JSON コンテンツタイプが有効になっています。

Command Modes ポリシーサーバ コンフィギュレーション (config-policy-server)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines JSON は、Cisco Identity Services Engine (ISE) からセキュリティ グループ アクセス コントロール リスト (SGACL) および環境データをダウンロードするためのコンテンツタイプとして使用されます。

Examples

次に、JSON コンテンツタイプを有効にする例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# content-type json
```

Related Commands	コマンド	説明
	cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。

cts authorization list

TrustSec シードデバイスで使用する認証、許可、およびアカウントिंग（AAA）サーバのリストを指定するには、Cisco TrustSec シードデバイスでグローバル コンフィギュレーション モードで **cts authorization list** コマンドを使用します。認証中にリストの使用を停止するには、このコマンドの **no** 形式を使用します。

cts authorization list *server_list*

no cts authorization list *server_list*

Syntax Description	<i>server_list</i> Cisco TrustSec AAA サーバグループ。
Command Default	なし
Command Modes	グローバル コンフィギュレーション (config)

サポートされるユーザロール

管理者 (Administrator)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、シードデバイスだけです。非シードデバイスは、TrustSec 環境データのコンポーネントとして TrustSec オーセンティケータのピアからの TrustSec AAA サーバリストを取得しません。

次の例は、TrustSec シードデバイスの AAA コンフィギュレーションを表示します。

```
Device# cts credentials id Device1 password Cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa authorization network MLIST group radius
Device(config)# cts authorization list MLIST
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Device(config)# radius-server vsa send authentication
Device(config)# dot1x system-auth-control
Device(config)# exit
```

Related Commands

コマンド	説明
show cts server-list	RADIUS サーバ設定を表示します。

cts change-password

ローカルデバイスと認証サーバの間でパスワードを変更するには、**cts change-password** 特権 EXEC コマンドを使用します。

```
cts change-password server ipv4_address udp_port {a-id hex_string | key radius_key }[source interface_list]
```

Syntax Description	server	認証サーバを指定します。
	ipv4_address	認証サーバの IP アドレス。
	udp_port	認証サーバの UDP ポート。
	a-id hex_string	ACS サーバの識別文字列を指定します。
	key	プロビジョニングに使用する RADIUS キーを指定します。
	source interface_list	(任意) 表示されるリストに従って、要求パケットの送信元アドレスのインターフェイスタイプとその識別パラメータを指定します。

Command Default なし

Command Modes 特権 EXEC (#)

サポートされるユーザロール
 管理者 (Administrator)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **cts change-password** コマンドにより、管理者は認証サーバを再設定しなくても、ローカルデバイスと Cisco Secure ACS 認証サーバ間で使用されるパスワードを変更することができます。

次に、スイッチと Cisco Secure ACS の間で Cisco TrustSec パスワードを変更する例を示します。

```
Device# cts change-password server 192.168.2.2 88 a-id ffef
```

cts credentials

ネットワークデバイスの TrustSec ID およびパスワードを指定するには、特権 EXEC モードで **cts credentials** コマンドを使用します。ログイン情報を削除するには、**clear cts credentials** コマンドを使用します。

cts credentials id *cts_id* **password** *cts_pwd*

Syntax Description	
credentials id <i>cts_id</i>	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときこのデバイスが使用する Cisco TrustSec デバイス ID を指定します。 <i>cts-id</i> 変数は、最大 32 文字で大文字と小文字を区別します。
password <i>cts_pwd</i>	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときこのデバイスが使用するパスワードを指定します。

Command Default なし

Command Modes 特権 EXEC (#)

サポートされるユーザロール
管理者 (Administrator)

Command History		変更内容
リリース		
Cisco IOS XE Fuji 16.9.2		このコマンドが導入されました。

Usage Guidelines



Important **cts credentials** コマンドは、特権 EXEC モードでのみ設定する必要があります。グローバル コンフィギュレーション (config) モードを使用して **cts credentials** コマンドを設定することはできません。

cts credentials コマンドは、EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときこのデバイスが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。Cisco TrustSec のログイン情報はスタートアップ コンフィギュレーションではなくキーストアに保存されているため、Cisco TrustSec のログイン情報の状態取得は不揮発性生成 (NVGEN) プロセスでは実行されません。デバイスは、Cisco Secure Access Control Server (ACS) から Cisco TrustSec アイデンティティを割り当てられるか、ACS から要求されたときに新しいパスワードを自動生成することができます。これらのログイン情報は、キーストアで保存され、実行コンフィギュレーションを保存する必要がなくなります。Cisco TrustSec デバイス ID を表示するには、**show cts credentials** コマンドを使用します。保存されたパスワードは表示されません。

デバイス ID またはパスワードを変更するには、コマンドを再入力します。キーストアをクリアするには、**clear cts credentials** コマンドを使用します。



Note Cisco TrustSec デバイス ID が変更された場合、Protected Access Credential (PAC) は古いデバイス ID に関連付けられており、新しいアイデンティティに対しては有効でないため、すべての PAC はキーストアから消去されます。

次に、Cisco TrustSec デバイス ID およびパスワードを設定する例を示します。

```
Device# cts credentials id cts1 password password1
CTS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

次に、Cisco TrustSec デバイス ID を cts_new、パスワードを password123 に変更する例を示します。

```
Device# cts credentials id cts_new password password123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y
```

```
TS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

次に、Cisco TrustSec デバイス ID およびパスワードの状態を表示する例を示します。

```
Device# show cts credentials

CTS password is defined in keystore, device-id = cts_new
```

Related Commands

コマンド	説明
clear cts credentials	Cisco TrustSec デバイス ID とパスワードをクリアします。
show cts credentials	現在の Cisco TrustSec デバイス ID およびパスワードの状態を表示します。
show cts keystore	ハードウェアおよびソフトウェアのキーストアの内容を表示します。

cts environment-data enable

REST アプリケーションプログラミング インターフェイス (API) による環境データのダウンロードを有効にするには、グローバル コンフィギュレーション モードで **cts environment-data enable** コマンドを使用します。環境データのダウンロードを無効にするには、このコマンドの **no** 形式を使用します。

cts environment-data enable
no cts environment-data enable

このコマンドには引数またはキーワードはありません。

Command Default

環境データのダウンロードは有効になっていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines

cts environment-data enable コマンドと **cts authorization list** コマンドを一緒に使用することはできません。**cts authorization list** コマンドでは、RADIUS による環境データのダウンロードが有効になります。

cts authorization list コマンドを使用して RADIUS ベースの設定を試行したときに **cts environment-data enable** コマンドがすでに設定されていると、コンソールに次のエラーメッセージが表示されます。

```
Error: 'cts policy-server or cts environment-data' related configs are enabled.
Disable http-based configs, to enable 'cts authorization'
```

Examples

次に、環境データのダウンロードを有効にする例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts environment-data enable
```

Related Commands

コマンド	説明
clear cts environment-data	環境データをクリアします。
debug cts environment-data	Cisco TrustSec 環境データ操作のデバッグを有効にします。
show cts environment-data	Cisco TrustSec の環境データ情報を表示します。

cts policy-server device-id

ポリシーサーバのデバイス ID を設定するには、グローバル コンフィギュレーション モードで **cts policy-server device-id** コマンドを使用します。ポリシーサーバのデバイス ID を削除するには、このコマンドの **no** 形式を使用します。

cts policy-server device-id *device-ID*
no cts policy-server device-id *device-ID*

Syntax Description	<i>device-ID</i>	Cisco TrustSec デバイスのデバイス ID。
---------------------------	------------------	------------------------------

Command Default	デバイス ID は設定されていません。
------------------------	---------------------

Command Modes	グローバル コンフィギュレーション (config)
----------------------	----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines	デバイス ID は、Cisco Identity Services Engine (ISE) でネットワーク アクセス デバイス (NAD) を追加するために使用したものと同等である必要があります。この ID は、Cisco ISE に環境データ要求を送信するために使用されます。
-------------------------	--

Examples

次に、ポリシーサーバのデバイス ID を設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server device-id server1
```

Related Commands	コマンド	説明
	cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバコンフィギュレーションモードを開始します。

cts policy-server name

Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバコンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **cts policy-server name** コマンドを使用します。ポリシーサーバを削除するには、このコマンドの **no** 形式を使用します。

cts policy-server name *server-name*
no cts policy-server name *server-name*

Syntax Description	<i>server-name</i>	ポリシーサーバ名。
Command Default	ポリシーサーバは設定されていません。	
Command Modes	グローバルコンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines ポリシーサーバ名にはすべての文字を使用できます。ポリシーサーバ名を設定すると、コンフィギュレーションモードがポリシーサーバコンフィギュレーションに切り替わります。このモードで、ポリシーサーバのその他の詳細を設定できます。

Examples

次に、ポリシーサーバ名を設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server name ISE1
Device(config-policy-server)#
```

Related Commands	コマンド	説明
	show cts policy-server	ポリシーサーバ情報を表示します。

cts policy-server order random

サーバ選択ロジックをランダム方式に変更するには、グローバルコンフィギュレーションモードで **cts policy-server order random** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

cts policy-server order random
no cts policy-server order random

このコマンドには引数またはキーワードはありません。

Command Default

デフォルトは順序どおりの選択です。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines

デバイスで複数の HTTP ポリシーサーバが設定されている場合、常に最初に設定されたサーバが選択されると、1つの Cisco Identity Services Engine (ISE) インスタンスが過負荷になる可能性があります。この状況を回避するには、各デバイスでランダムにサーバを選択します。ランダムな番号がデバイスによって生成され、この番号に基づいてサーバが選択されます。デバイスごとにランダムな番号を生成するには、デバイスの一意のボード ID と Cisco TrustSec プロセス ID を使用して乱数ジェネレータを初期化します。

サーバ選択ロジックをランダム方式に変更するには、**cts policy-server order random** コマンドを使用します。このコマンドが選択されていない場合、デフォルトの順序どおりの選択が使用されます。

順序どおりの選択では、サーバが設定された順序（パブリックサーバリスト）またはダウンロードされた順序（プライベートサーバリスト）で選択されます。サーバが選択されると、そのサーバがデッド状態としてマークされるまで使用され、その後リストの次のサーバが選択されます。

Examples

次に、サーバ選択ロジックを変更する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server order random
```

Related Commands

コマンド	説明
cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバコンフィギュレーションモードを開始します。

cts policy-server username

ポリシーサーバのユーザ名を設定するには、グローバル コンフィギュレーション モードで **cts policy-server username** コマンドを使用します。ポリシーサーバのユーザ名を削除するには、このコマンドの **no** 形式を使用します。

cts policy-server username *username***password** {**0** | **6** | **7** *password*}*password*
no cts policy-server username

Syntax Description		
	<i>username</i>	REST アプリケーション プログラミング インターフェイス (API) にアクセスするためのユーザ名。
	password	ユーザの認証で使用するパスワードを指定します。
	0	暗号化されていないパスワードを指定します。
	6	暗号化パスワードを指定します。
	7	非表示のパスワードを指定します。
	<i>password</i>	暗号化または非暗号化パスワード。

Command Default ユーザログイン情報は設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines デバイスで設定する前に、Cisco Identity Services Engine (ISE) でユーザ名とパスワードを REST API アクセス用のログイン情報として設定しておく必要があります。詳細については、「Cisco TrustSec Policies Configuration」の章の「TrustSec HTTP Servers」セクションを参照してください。

Examples

次に、ポリシーサーバのログイン情報を設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server username user1 password 0 ise-password
```

Related Commands

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。

cts refresh

すべてまたは特定の Cisco TrustSec ピアの TrustSec ピア認証ポリシーをリフレッシュするか、認証サーバによりデバイスにダウンロードされた SGACL ポリシーをリフレッシュするには、特権 EXEC モードで **cts refresh** コマンドを使用します。

```
cts refresh {peer [peer_id] | sgt [sgt_number | default | unknown]}
```

Syntax Description

environment-data 環境データをリフレッシュします。

peer Peer-ID (任意) peer-id が指定される場合、指定されたピア接続に関連するポリシーだけがリフレッシュされます。

sgt sgt_number (任意) 認証サーバからの SGACL ポリシーの即時リフレッシュを実行します。SGT 番号が指定されている場合、その SGT に関連するポリシーだけがリフレッシュされます。

default (任意) デフォルトの SGACL ポリシーをリフレッシュします。

unknown (任意) 未知の SGACL ポリシーをリフレッシュします。

Command Default

なし

Command Modes

特権 EXEC (#)

サポートされるユーザロール

管理者 (Administrator)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

すべての TrustSec ピアのピア認証ポリシーをリフレッシュするには、ピア ID を指定しないで **cts policy refresh** を入力します。

ピア認可ポリシーは EAP-FAST NDAC 認証の成功の最後に Cisco ACS から最初にダウンロードされます。Cisco ACS はピア認証ポリシーを更新するように設定されていますが、**cts policy refresh** コマンドにより、Cisco ACS タイマーが期限切れになる前にポリシーの即時更新を強制できます。このコマンドは、セキュリティグループタグ (SGT) を適用でき、セキュリティグループアクセスコントロールリスト (SGACL) を強制できる TrustSec デバイスだけに関連します。

次に、すべてのピアの TrustSec ピア認証ポリシーをリフレッシュする例を示します。

```
Device# cts policy refresh
Policy refresh in progress
```

次に、すべてのピアの TrustSec ピア認証ポリシーを表示する出力例を示します。

```
VSS-1# show cts policy peer
```

```
CTS Peer Policy
=====
device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

Related Commands

コマンド	説明
clear cts policy	Cisco TrustSec ポリシーをすべてクリアするか、ピア ID または SGT によりクリアします。
show cts policy peer	すべてまたは特定の TrustSec ピアのピア認可ポリシーが表示されます。

cts rekey

セキュリティアソシエーションプロトコル（SAP）で使用するペアワイズマスターキーを再生成するには、**cts rekey** 特権 EXEC コマンドを使用します。

cts rekey interface type slot/port

Syntax Description

interface type slot/port SAP キーを再生成する Cisco TrustSec インターフェイスを指定します。

Command Default

なし

Command Modes

特権 EXEC (#)

サポートされるユーザロール
管理者（Administrator）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

SAP のペアワイズマスターキー（PMK）のリフレッシュは通常、ネットワークイベントおよび dot1X 認証に関連する設定不可能な内部タイマーの組み合わせによりトリガーされ、自動的に行われます。暗号キーを手動で更新する機能は、多くの場合、ネットワークアドミニストレーションのセキュリティ要件の一部です。手動で PMK のリフレッシュを強制するには、**cts rekey** コマンドを使用します。

TrustSec は、dot1X 認証でスイッチ間のリンク間暗号化を作成する必要のない手動コンフィギュレーションモードをサポートします。この場合、PMK は、**sap pmk** Cisco TrustSec 手動インターフェイスコンフィギュレーションコマンドを使用してリンクの両端のデバイスで手動で設定されます。

次に、指定したインターフェイス上で PMK を再生成する例を示します。

```
Device# cts rekey interface gigabitEthernet 2/1
```

Related Commands

コマンド	説明
sap mode-list (cts manual)	手動モードの Cisco TrustSec SAP を設定します。

cts role-based enforcement

Cisco TrustSec を使用したロールベースのアクセス制御をグローバルおよび特定のレイヤ 3 インターフェイスで有効にするには、グローバルコンフィギュレーションモードおよびインターフェイス コンフィギュレーション モードで **cts role-based enforcement** コマンドをそれぞれ使用します。ロールベースのアクセス制御のインターフェイスレベルでの適用を無効にするには、このコマンドの **no** 形式を使用します。

cts role-based enforcement
no cts role-based enforcement

Syntax Description	このコマンドにはキーワードまたは引数はありません。				
Command Default	ロールベースのアクセス制御のインターフェイスレベルでの適用はグローバルに無効になっています。				
Command Modes	グローバル コンフィギュレーション (config) インターフェイス コンフィギュレーション (config-if)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines グローバル コンフィギュレーションモードで **cts role-based enforcement** コマンドを使用すると、ロールベースのアクセス制御がグローバルに有効になります。ロールベースのアクセス制御がグローバルに有効になると、デバイスのすべてのレイヤ 3 インターフェイスで自動的に有効になります。特定のレイヤ 3 インターフェイスでロールベースのアクセス制御を無効にするには、インターフェイス コンフィギュレーションモードでこのコマンドの **no** 形式を使用します。インターフェイス コンフィギュレーションモードで **cts role-based enforcement** コマンドを使用すると、特定のレイヤ 3 インターフェイスでロールベースのアクセス制御の適用が可能になります。

属性ベースのアクセス制御リストでは、ネットワークデバイスの Cisco TrustSec アクセス制御を整理して管理します。セキュリティ グループ アクセス コントロール リスト (SGACL) は、セキュリティグループタグ (SGT) の値に基づいてアクセスをフィルタ処理するためのレイヤ 3/4 アクセス制御リストです。通常、フィルタ処理は Cisco TrustSec ドメインの出力ポートで実行されます。ロールベースのアクセス制御リスト (RBACL) と SGACL という用語は同じ意味で使用され、どちらも属性ベースのアクセス制御 (ABAC) ポリシーモデルで使用されるトポロジに依存しない ACL を示します。

次に、ギガビットイーサネット インターフェイスでロールベースのアクセス制御を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
```

```
Device(config-if)# cts role-based enforcement  
Device(config-if)# end
```

cts role-based l2-vrf

レイヤ 2 VLAN の Virtual Routing and Forwarding (VRF) インスタンスを選択するには、グローバル コンフィギュレーション モードで **cts role-based l2-vrf** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [,] [-]
no cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [,] [-]
```

Syntax Description

<i>vrf-name</i>	VRF インスタンスの名前。
vlan-list	VRF インスタンスに割り当てられる VLAN のリストを指定します。
all	すべての VLAN を指定します。
<i>vlan-ID</i>	VLAN ID。有効な値は 1 ~ 4094 です。
,	(任意) 別の VLAN をカンマで区切って指定します。
-	(任意) VLAN の範囲をハイフンで区切って指定します。

Command Default

VRF インスタンスは選択されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

vlan-list 引数には単一の VLAN ID、カンマで区切られた VLAN ID のリスト、またはハイフンで区切られた VLAN ID の範囲を指定できます。

all キーワードは、ネットワークデバイスによってサポートされている VLAN の全範囲と同等です。**all** キーワードは、不揮発性生成 (NVGEN) プロセスで保持されません。

cts role-based l2-vrf コマンドが同じ VRF に複数回実行される場合、入力される連続した各コマンドは、指定された VRF に VLAN ID を追加します。

cts role-based l2-vrf コマンドで設定された VRF 割り当ては、VLAN がレイヤ 2 VLAN として維持されている間はアクティブです。VRF の割り当てがアクティブな間に、学習した IP-SGT バインディングも VRF と IP プロトコルバージョンに関連付けられた転送情報ベース (FIB) テーブルに追加されます。VLAN のスイッチ仮想インターフェイス (SVI) がアクティブになると、VRF から VLAN への割り当てが非アクティブになり、VLAN で学習されたすべてのバインディングが SVI の VRF に関連付けられた FIB テーブルに移動されます。

SVI インターフェイスを設定するには **interface vlan** コマンドを使用し、VRF インスタンスをインターフェイスに関連付けるには **vrf forwarding** コマンドを使用します。

VRF から VLAN への割り当ては、割り当てが非アクティブになっても保持されます。SVI が削除された、または SVI の IP アドレスの変更された場合に再アクティブ化されます。再アクティブ化された場合、IP-SGT バインディングは、SVI の FIB に関連付けられた FIB テーブルから、**cts role-based l2-vrf** コマンドによって割り当てられた VRF に関連付けられた FIB テーブルに戻されます。

次に、VRF インスタンスに割り当てられる VLAN のリストを選択する例を示します。

```
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

次に、SVI インターフェイスを設定し、VRF インスタンスを関連付ける例を示します。

```
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf1
```

Related Commands

コマンド	説明
interface vlan	VLAN インターフェイスを設定します。
vrf forwarding	VRF インスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。
show cts role-based permissions	SGACL の権限リストを表示します。

cts role-based monitor

ロールベース（セキュリティグループ）アクセスリストモニタリングを有効にするには、グローバルコンフィギュレーションモードで **cts role-based monitor** コマンドを使用します。ロールベースアクセスリストモニタリングを削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based monitor {all | permissions {default [ipv4 | ipv6] | from {sgt | unknown} to {sgt | unknown} [ipv4 | ipv6]}}
no cts role-based monitor {all | permissions {default [ipv4 | ipv6] | from {sgt | unknown} to {sgt | unknown} [ipv4 | ipv6]}}
```

Syntax Description	all	permissions	default	ipv4	ipv6	from	sgt	unknown
	すべての宛先タグへのすべての送信元タグの権限をモニタします。	1つの送信元タグから1つの宛先タグへの権限をモニタします。	デフォルトの権限リストをモニタします。	(任意) IPv4 プロトコルを指定します。	(任意) IPv6 プロトコルを指定します。	フィルタリングされるトラフィックの送信元グループタグを指定します。	セキュリティグループタグ (SGT) 有効値は 2 ~ 65519 です。	未知の送信元または宛先グループタグ (DST) を指定します。

Command Default ロールベース アクセス コントロール モニタリングは有効になっていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines グローバルモニタモードを有効にするには、**cts role-based monitor all** コマンドを使用します。**cts role-based monitor all** コマンドが設定されている場合、**show cts role-based permissions** コマンドの出力には、設定されているすべてのポリシーのモニタモードが **true** と表示されます。

次に、送信元タグから宛先タグへの SGACL モニタを設定する例を示します。

```
Device(config)# cts role-based monitor permissions from 10 to 11
```

Related Commands

コマンド	説明
show cts role-based permissions	SGACLの権限リストを表示します。

cts role-based permissions

1つの送信元グループから1つの宛先グループへの権限を有効にするには、グローバルコンフィギュレーションモードで **cts role-based permissions** コマンドを使用します。権限を削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based permissions {default | from {sgt | unknown}to {sgt | unknown}} {rbacl-name |
ipv4 | ipv6}
no cts role-based permissions {default | from {sgt | unknown}to {sgt | unknown}} {rbacl-name |
ipv4 | ipv6}
```

Syntax Description	default
	デフォルトの権限リストを指定します。セキュリティグループアクセスコントロールリスト (SGACL) 権限が静的または動的に設定されていないすべてのセル (SGT ペア) は、デフォルトのカテゴリに属します。
	from フィルタリングされるトラフィックの送信元グループタグを指定します。
	sgt セキュリティグループタグ (SGT) 有効値は 2 ~ 65519 です。
	unknown 未知の送信元または宛先グループタグを指定します。
	rbacl-name ロールベース アクセス コントロール リスト (RBACL) または SGACL の名前。この設定では最大 16 の SGACL を指定できます。
	ipv4 IPv4 プロトコルを指定します。
	ipv6 IPv6 プロトコルを指定します。

Command Default 1つの送信元グループから1つの宛先グループへの権限は有効になっていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 特定の送信元グループタグ (SGT)、宛先グループタグ (DGT) ペアの SGACL のリストを定義したり、置き換えたり、削除したりするには、**cts role-based permissions** コマンドを使用します。このポリシーは、同じ DGT または SGT に対するダイナミックなポリシーがないかぎり有効です。

cts role-based permissions default コマンドでは、同じ DGT に対するダイナミックなポリシーがないかぎり、デフォルトポリシーの SGACL のリストを定義したり、置き換えたり、削除したりすることができます。

次に、宛先グループの権限を有効にする例を示します。

```
Device(config)# cts role-based permissions from 6 to 6 mon_2
```

Related Commands

コマンド	説明
show cts role-based permissions	SGACLの権限リストを表示します。

cts role-based sgt-caching

セキュリティグループタグ（SGT）キャッシングをグローバルに有効にするには、グローバル コンフィギュレーションモードで **cts role-based sgt-caching** コマンドを使用します。SGT キャッシングを削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based sgt-caching [vlan-list {vlan-id | all}]
no cts role-based sgt-caching [vlan-list {vlan-id | all}]
```

Syntax Description	vlan-list <i>vlan-id</i>	(任意) VLAN ID を指定します。各 VLAN ID はカンマで区切られ、ID の範囲はハイフンで指定されます。有効な値は 1 ～ 4094 です。
	all	(任意) すべての VLAN を選択します。

Command Default SGT キャッシングは設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines VLAN で SGT キャッシングを有効にするには、**cts role-based sgt-caching** コマンドと **cts role-based sgt-caching vlan-list** コマンドの両方を設定する必要があります。

例

次に、VLAN で SGT キャッシングを有効にする例を示します。

```
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# cts role-based sgt-caching vlan-list 4
```

cts role-based sgt-map

ホストまたは VRF のいずれかで送信元 IP アドレスをセキュリティグループタグ (SGT) に手動でマッピングするには、グローバルコンフィギュレーションモードで **cts role-based sgt-map** コマンドを使用します。マッピングを削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based sgt-map {ipv4_netaddress | ipv6_netaddress | ipv4_netaddress/prefix | ipv6_netaddress/prefix}
sgt sgt-number
cts role-based sgt-map host {ipv4_hostaddress | ipv6_hostaddress} sgt sgt-number
cts role-based sgt-map vlan-list [vlan_ids | all] sgt sgt-number
cts role-based sgt-map vrf instance_name
{ipv4_netaddress | ipv6_netaddress | ipv4_netaddress/prefix | ipv6_netaddress/prefix | host
{ipv4_hostaddress | ipv6_hostaddress}} sgt sgt-number
no cts role-based sgt-map
```

Syntax Description		
ipv4_netaddress ipv6_netaddress		SGT に関連付けるネットワークを指定します。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
ipv4_netaddress/prefix ipv6_netaddress/prefix		指定したサブネットアドレス (IPv4 または IPv6) のすべてのホストに SGT をマッピングします。IPv4 はドット付き 10 進数 CIDR 表記で、IPv6 はコロン 16 進数表記で指定されます。
host { <i>ipv4_hostaddress</i> <i>ipv6_hostaddress</i> }		指定したホスト IP アドレスを SGT とバインドします。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
vlan-list { <i>vlan_ids</i> all }		VLAN ID を指定します。 <ul style="list-style-type: none"> (任意) <i>vlan_ids</i>: 各 VLAN ID はカンマで区切られ、ID の範囲はハイフンで指定されます。 (任意) all: すべての VLAN ID を指定します。
vrf <i>instance_name</i>		以前デバイスで作成した VRF インスタンスを指定します。
sgt <i>sgt-number</i>		SGT 番号 (0 ~ 65,535) を指定します。

Command Default なし

Command Modes グローバル コンフィギュレーション (config)

Command History		
	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

自動的に SGT を送信元 IP アドレスにマッピングするための、Cisco Identity Services Engine、Cisco Secure ACS、ダイナミックアドレス解決プロトコル (ARP) インスペクション、動的ホスト制御プロトコル (DHCP) スヌーピング、ホストトラッキングが使用できない場合、**cts role-based sgt-map** コマンドを使用して SGT を次の内容にマッピングできます。

- 単一ホストの IPv4 または IPv6 アドレス
- IPv4 または IPv6 ネットワークまたはサブネットワーク上のすべてのホスト
- VRF
- 単一または複数の VLAN

cts role-based sgt-map コマンドは、指定されたネットワークアドレス範囲内のパケットに、指定された SGT をバインドします。

SXP は指定されたネットワークまたはサブネットワーク内のすべての可能な個別 IP-SGT バインディングの包括的な拡張をエクスポートします。IPv6 バインディングとサブネットバインディングは SXP バージョン 2 以降の SXP リスナー ピアだけにエクスポートされます。拡張には、個別に認識されたホストバインディングや、ネストされたサブネットバインディングに対して SXP から設定または学習されたホストバインディングは含まれません。

cts role-based sgt-map host コマンドは、IP 送信元アドレスが指定ホストアドレスで一致した場合に、この着信パケットに指定 SGT をバインドします。この IP-SGT バインディングは優先順位が最も低く、他の送信元から動的に検出されたその他のバインディング (SXP またはローカルで認証済みホストなど) が存在する場合は無視されます。バインディングは、SGT インポジションおよび SGACL 強制用にデバイス上でローカルに使用されます。このバインディングが指定したホスト IP アドレスに認識される唯一のバインディングである場合、これが SXP ピアにエクスポートされます。

vrf キーワードは、以前に **vrf definition** グローバル コンフィギュレーション コマンドで定義された仮想ルーティングおよびフォワーディングテーブルを指定します。**cts role-based sgt-map vrf** グローバル コンフィギュレーション コマンドで指定された IP-SGT バインディングは、指定された VRF と、入力された IP アドレスのタイプによって示される IP プロトコルのバージョンに関連付けられた IP-SGT のテーブルに入力されます。

cts role-based sgt-map vlan-list コマンドは、SGT を指定された VLAN または VLAN のセットにバインドします。キーワード **all** は、デバイスでサポートされている VLAN の全範囲と同じで、揮発性生成 (NVGEN) プロセスで保持されません。指定 SGT は指定した VLAN のいずれかで受信した着信パケットにバインドされます。システムでは、DHCP/ARP スヌーピング (別名 IP デバイストラッキング) などの検出方式を使用して、このコマンドによってマッピングされた VLAN のいずれかでアクティブなホストを検出します。また、各 VLAN の SVI に関連付けられたサブネットを指定された SGT にマッピングすることもできます。SXP は、バインディングのタイプに応じて、結果のバインディングをエクスポートします。

Examples

次に、送信元 IP アドレスを SGT に手動でマッピングする例を示します。

```
Device(config)# cts role-based sgt-map 10.10.1.1 sgt 77
```

次の例では、デバイスでホスト IP アドレス 10.1.2.1 を SGT 3 にバインドし、10.1.2.2 を SGT 4 にバインドしています。これらのバインディングは、SXP によって SGACL 強制のデバイスに転送されます。

```
Device(config)# cts role-based sgt-map host 10.1.2.1 sgt 3
Device(config)# cts role-based sgt-map host 10.1.2.2 sgt 4
```

Related Commands

コマンド	説明
show cts role-based sgt-map	ロールベースのアクセス制御の情報を表示します。

cts sxp connection peer

Cisco TrustSec セキュリティグループタグ交換プロトコルのピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定し、リスナーまたはスピーカーデバイスのグローバルなホールド時間を指定し、接続が双方向であるかどうかを指定するには、グローバル コンフィギュレーションモードで **cts sxp connection peer** コマンドを使用します。これらのピア接続の設定を削除するには、このコマンドの **no** 形式を使用します。

```
cts sxp connection peer ipv4-address {source | password} {default | none} mode {local | peer} [[[listener | speaker] [hold-time minimum-time maximum-time | vrf vrf-name ]] | both [vrf vrf-name ]]
```

```
cts sxp connection peer ipv4-address {source | password} {default | none} mode {local | peer} [[[listener | speaker] [hold-time minimum-time maximum-time | vrf vrf-name ]] | both [vrf vrf-name ]]
```

Syntax Description

<i>ipv4-address</i>	SXP ピアの IPv4 アドレス。
source	送信元の IPv4 アドレスを指定します。
password	ピア接続に SXP パスワードを使用するように指定します。
default	デフォルトの SXP パスワードを使用するように指定します。
none	パスワードを使用しないように指定します。
mode	ローカルまたはピアのいずれかの SXP 接続モードを指定します。
local	SXP 接続モードでローカルデバイスを参照するように指定します。
peer	SXP 接続モードでピアデバイスを参照するように指定します。
listener	(任意) デバイスを接続のリスナーとして指定します。
speaker	(任意) デバイスを接続のスピーカーとして指定します。
hold-time <i>minimum-time</i> <i>maximum-time</i>	(任意) デバイスのホールド時間を秒単位で指定します。最小時間と最大時間の範囲は 0 ~ 65535 です。 <i>maximum-time</i> の値は、キーワード peer speaker および local listener を使用する場合のみ必要です。それ以外の場合は、 <i>minimum-time</i> の値のみが必要です。 Note 最小時間と最大時間の両方が必要な場合、 <i>maximum-time</i> の値を <i>minimum-time</i> の値以上にする必要があります。
vrf <i>vrf-name</i>	(任意) ピアに対する Virtual Routing and Forwarding (VRF) インスタンス名を指定します。

both	(任意) デバイスを双方向 SXP 接続のスピーカーとリスナーの両方として指定します。
-------------	---

Command Default CTS-SXP ピア IP アドレスは設定されておらず、ピア接続に CTS-SXP ピアパスワードは使用されません。

CTS-SXP 接続パスワードのデフォルトの設定は **none** です。

Command Modes グローバル コンフィギュレーション (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ピアへの CTS-SXP 接続が **cts sxp connection peer** コマンドを使用して設定された場合、接続モードだけを変更できます。**vrf** キーワードはオプションです。**VRF** 名が指定されていない、または **VRF** 名が **default** キーワードで指定されている場合、接続はデフォルトルーティングまたはフォワーディングドメインで設定されます。

hold-time maximum-period の値は、キーワード **peer speaker** および **local listener** を使用する場合があります。それ以外の場合は、**hold-time minimum-period** の値のみが必要です。



Note *maximum-period* 値は、*minimum-period* 値よりも大きい必要はありません。

双方向 SXP 接続を設定するには、**both** キーワードを使用します。双方向 SXP の設定をサポートすることで、ピアはスピーカーとリスナーのどちらとしても動作し、単一の接続を使用する双方向の SXP バインドを伝播できるようになります。

Examples

次に、CTS-SXP をイネーブルにし、Device_A (スピーカー) で Device_B (リスナー) への SXP ピア接続を設定する例を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B (リスナー) で Device_A (スピーカー) への CTS-SXP ピア接続を設定する例を示します。

```
Device_B> enable
Device_B# configure terminal
Device_B#(config)# cts sxp enable
Device_B#(config)# cts sxp default password Cisco123
Device_B#(config)# cts sxp default source-ip 10.20.2.2
```

```
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

SXP 接続のピアと送信元の両方の IP アドレスを設定することもできます。 **cts sxp connection** コマンドで送信元 IP アドレスを指定すると、デフォルト値が上書きされます。

```
Device_A(config)# cts sxp connection peer 51.51.51.1 source 51.51.51.2 password none mode local speaker
```

```
Device_B(config)# cts sxp connection peer 51.51.51.2 source 51.51.51.1 password none mode local listener
```

次の例は、双方向 CTS-SXP を有効化し、Device_A 上の SXP ピア接続が Device_B に接続するよう設定する方法を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

Related Commands

コマンド	説明
cts sxp default password	Cisco TrustSec SXP のデフォルトパスワードを設定します。
cts sxp default source-ip	Cisco TrustSec SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで Cisco TrustSec SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	Cisco TrustSec SXP の復帰期間を変更します。
cts sxp retry	Cisco TrustSec SXP の再試行期間タイマーを変更します。
cts sxp speaker hold-time	Cisco TrustSec SGT SXPv4 ネットワークにおけるスピーカーデバイスのグローバルなホールド時間を設定します。
cts sxp listener hold-time	Cisco TrustSec SGT SXPv4 ネットワークにおけるリスナーデバイスのグローバルなホールド時間を設定します。
show cts sxp	Cisco TrustSec SXP のすべての設定のステータスを表示します。

cts sxp default password

Cisco TrustSec セキュリティグループタグ (SGT) 交換プロトコル (CTS-SXP) のデフォルトパスワードを指定するには、グローバル コンフィギュレーション モードで **cts sxp default password** コマンドを使用します。CTS-SXP のデフォルトパスワードを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default password {0 unencrypted-pwd | 6 encrypted-key | 7 encrypted-keycleartext-pwd}
no cts sxp default password {0 unencrypted-pwd | 6 encrypted-key | 7 encrypted-keycleartext-pwd}

Syntax Description

0 <i>unencrypted-pwd</i>	暗号化されていない CTS-SXP デフォルトパスワードが続くことを指定します。パスワードの最大長は 32 文字です。
6 <i>encrypted-key</i>	タイプ 6 暗号化パスワードを CTS SXP デフォルトパスワードとして使用することを指定します。パスワードの最大長は 32 文字です。
7 <i>encrypted-key</i>	タイプ 7 暗号化パスワードを CTS SXP デフォルトパスワードとして使用することを指定します。パスワードの最大長は 32 文字です。
<i>cleartext-pwd</i>	クリアテキストの CTS-SXP デフォルトパスワードを指定します。パスワードの最大長は 32 文字です。

Command Default

タイプ 0 (クリアテキスト)

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

cts sxp default password コマンドは、デバイスに設定されているすべての SXP 接続に任意で使用する CTS-SXP デフォルトパスワードを設定します。CTS-SXP パスワードは、クリアテキストまたは 0、7、6 暗号化タイプキーワードを使用して暗号化したものを使用します。暗号化タイプが 0 の場合は、暗号化されていないクリアテキストパスワードが続きます。

Examples

次に、CTS-SXP をイネーブルにし、Device_A (スピーカー) で Device_B (リスナー) への SXP ピア接続を設定する例を示します。

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）でDevice_A（スピーカー）へのCTS-SXPピア接続を設定する例を示します。

```
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

Related Commands

コマンド	説明
cts sxp connection peer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	SXP のすべての設定のステータスを表示します。

cts sxp default source-ip

Cisco TrustSec セキュリティグループタグ (SGT) 交換プロトコル (CTS-SXP) の送信元 IPv4 アドレスを設定するには、グローバル コンフィギュレーション モードで **cts sxp default source-ip** コマンドを使用します。CTS-SXP のデフォルトの送信元 IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
cts sxp default source-ip ipv4-address
no cts sxp default source-ip ipv4-address
```

Syntax Description

<i>ip-address</i>	CTS-SXP のデフォルトの送信元 IPv4 アドレス。
-------------------	-------------------------------

Command Default

CTS-SXP の送信元 IP アドレスは設定されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

cts sxp default source-ip コマンドは、送信元 IP アドレスが指定されていない場合に、CTS-SXP が新規の TCP 接続すべてに使用するデフォルトの送信元 IP アドレスを設定します。既存の TCP 接続は、このコマンドが入力されても影響を受けません。CTS-SXP 接続は 3 つのタイマーによって制御されます。

- 再試行タイマー
- 削除のホールドダウン タイマー
- 復帰タイマー

Examples

次に、CTS-SXP をイネーブルにし、Device_A (スピーカー) で Device_B (リスナー) への SXP ピア接続を設定する例を示します。

```
Device_A# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B (リスナー) で Device_A (スピーカー) への CTS-SXP ピア接続を設定する例を示します。

```
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
```

```
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

Related Commands

コマンド	説明
cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルトパスワードを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のログを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	SXP のすべての設定のステータスを表示します。

cts sxp filter-enable

フィルタリストおよびフィルタグループの作成後にフィルタリングを有効にするには、グローバル コンフィギュレーション モードで **cts sxp filter-enable** コマンドを使用します。フィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

```
cts sxp filter-enable
no cts sxp filter-enable
```

Syntax Description

このコマンドにはキーワードまたは引数はありません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、フィルタリングを有効または無効にするためにいつでも使用できます。設定したフィルタリストとフィルタグループは、フィルタリングを有効にした後にのみフィルタリングの実装に使用できます。フィルタアクションでは、フィルタリングを有効にした後に交換されたバインディングのみがフィルタリングされます。フィルタリングを有効にする前に交換されたバインディングに対しては効果はありません。

Examples

```
Device(config)# cts sxp filter-enable
```

Related Commands

コマンド	説明
cts sxp filter-list	IP プレフィックス、SGT、またはその両方の組み合わせに基づいて IP-SGT バインディングをフィルタリングするための SXP フィルタリストを作成します。
cts sxp filter-group	一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成します。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp filter-group

一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成するには、グローバル コンフィギュレーション モードで **cts sxp filter-group** コマンドを使用します。フィルタグループを削除するには、このコマンドの **no** 形式を使用します。

```
cts sxp filter-group {listener | speaker} {filter-group-name | global filter-list-name}
no cts sxp filter-group {listener | speaker} {filter-group-name | global filter-list-name}
```

Syntax Description

listener	一連のリスナーのフィルタグループを作成します。
speaker	一連のスピーカーのフィルタグループを作成します。
global	デバイスのすべてのスピーカーまたはリスナーをグループ化します。
<i>filter-group-name</i>	フィルタグループの名前。
<i>filter-list-name</i>	フィルタ リストの名前。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを発行すると、デバイスがフィルタ グループ コンフィギュレーション モードになります。このモードで、グループ化するデバイスを指定し、フィルタグループにフィルタリストを適用できます。

デバイスまたはピアをグループに追加するためのコマンドの形式は次のとおりです。

peer ipv4 peer-IP

1つのコマンドで1つのピアを追加できます。ピアをさらに追加するには、必要な回数だけコマンドを繰り返します。

フィルタリストをグループに適用するためのコマンドの形式は次のとおりです。

filter filter-list-name

グローバルリスナーおよびグローバルスピーカーのフィルタグループオプションではピアリストは指定できません。この場合、フィルタはすべての SXP 接続に適用されます。

グローバルなフィルタグループとピアベースのフィルタグループの両方が適用されている場合、グローバルフィルタが優先されます。グローバルリスナーまたはグローバルスピーカーのいずれかのフィルタグループのみが設定されている場合、その方向でのみグローバルフィルタリングが優先されます。もう一方の方向については、ピアベースのフィルタグループが実装されます。

Examples

次に、**group_1** というリスナーグループを作成し、そのグループにピアとフィルタリストを割り当てる例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# filter filter_1
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

次に、**group_2** というグローバルリスナーグループを作成する例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

Related Commands

コマンド	説明
cts sxp filter-list	IP プレフィックス、SGT、またはその両方の組み合わせに基づいて IP-SGT バインディングをフィルタリングするための SXP フィルタリストを作成します。
cts sxp filter-enable	フィルタリングを有効にします。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp filter-list

IP-SGT バインディングをフィルタリングするための一連のフィルタルールを保持する SXP フィルタリストを作成するには、グローバル コンフィギュレーション モードで **cts sxp filter-list** コマンドを使用します。フィルタリストを削除するには、このコマンドの **no** 形式を使用します。

```
cts sxp filter-list filter-list-name
no cts sxp filter-list filter-list-name
```

Syntax Description

<i>filter-list-name</i>	フィルタリストの名前。
-------------------------	-------------

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを発行すると、デバイスがフィルタ リスト コンフィギュレーション モードになります。このモードで、フィルタリストのルールを指定できます。

フィルタルールは、SGT、IP プレフィックス、または SGT と IP プレフィックスの両方の組み合わせに基づいて設定できます。

グループにルールを追加するためのコマンドの形式は次のとおりです。

```
sequence-number action(permit/deny) filter-type(ipv4/ipv6/sgt) value/values
```

たとえば、SGT 値が 20 である SGT-IP バインディングを許可するルールは次のようになります。

```
30 permit sgt 20
```

シーケンス番号はオプションです。シーケンス番号を指定しない場合は、システムによって生成されます。シーケンス番号は、最後に使用/設定されたシーケンス番号から自動的に 10 ずつ増分されます。2 つの既存のルールの間のシーケンス番号を指定することによって新しいルールを挿入できます。

有効な SGT 値の範囲は 2 ~ 65519 です。1 つのルールに複数の SGT 値を指定するには、スペースを使用して値を区切ります。1 つのルールに最大 8 つの SGT 値を指定できます。

SGT と IP プレフィックスを組み合わせられたルールでは、ルールの両方の部分にバインディングの一致がある場合、ルールの 2 つ目の部分で指定されたアクションが優先されます。たとえば、次のルールでは、IP プレフィックス 10.0.0.1 の SGT 値が 20 の場合、ルールの最初の部分でバインディングが許可されても、対応するバインディングが拒否されます。

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

同様に、次のルールでは、IP プレフィックス 10.0.0.1 の SGT が 20 で最初のアクションではバインディングが許可されなくても、SGT 値 20 のバインディングが許可されます。

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

Examples

次に、フィルタリストを作成していくつかのルールを追加する例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device (config-filter-list)# 10 deny ipv4 10.0.0.1/24 permit sgt 100
Device(config-filter-list)# 20 permit sgt 60 61 62 63
```

Related Commands

コマンド	説明
cts sxp filter-enable	SXP の IP プレフィックスおよび SGT ベースのフィルタリングを有効にします。
cts sxp filter-group	一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成します。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp log binding-changes

IP と Cisco TrustSec セキュリティグループタグ (SGT) 交換プロトコル (CTS-SXP) のバインディングの変更のロギングを有効にするには、グローバル コンフィギュレーション モードで **cts sxp log binding-changes** コマンドを使用します。ロギングを無効にするには、このコマンドの **no** 形式を使用します。

```
cts sxp log binding-changes
no cts sxp log binding-changes
```

Command Default ロギングは無効になっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **cts sxp log binding-changes** コマンドを使用すると、IP と SGT のバインディングの変更のロギングが有効になります。IP アドレスと SGT のバインディングに追加、削除、変更が発生するたびに SXP の syslog (sev 5 syslog) が生成されます。これらの変更は SXP 接続で学習されて伝播されません。

Related Commands	コマンド	説明
	cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
	cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
	cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
	cts sxp enable	デバイスで CTS-SXP を有効にします。
	cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
	cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
	show cts sxp	すべての SXP 設定のステータスを表示します。

cts sxp reconciliation period

Cisco TrustSec セキュリティグループタグ (SGT) 交換プロトコル (CTS-SXP) の復帰期間を変更するには、グローバル コンフィギュレーション モードで **cts sxp reconciliation period** コマンドを使用します。CTS-SXP の復帰期間をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cts sxp reconciliation period *seconds*
no cts sxp reconciliation period *seconds*

Syntax Description

<i>seconds</i>	CTS-SXP 復帰タイマー (秒)。範囲は 0 ~ 64000 です。デフォルトは 120 です。
----------------	--

Command Default

120 秒 (2 分)

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ピアが CTS-SXP 接続を終了すると、内部の削除ホールドダウンタイマーが開始されます。削除ホールドダウンタイマーが終了する前にピアが再接続すると、CTS-SXP 復帰タイマーが開始されます。CTS-SXP 復帰期間タイマーがアクティブな間、CTS-SXP ソフトウェアは前回の接続で学習した SGT マッピングエントリを保持し、無効なエントリを削除します。SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

Related Commands

コマンド	説明
cts sxp connection peer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のログギングをオンにします。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	CTS-SXP のすべての設定のステータスを表示します。

cts sxp retry period

Cisco TrustSec セキュリティグループタグ (SGT) 交換プロトコル (CTS-SXP) の再試行期間タイマーを変更するには、グローバル コンフィギュレーション モードで **cts sxp retry period** コマンドを使用します。CTS-SXP の再試行期間タイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cts sxpretry period *seconds*
no cts sxpretry period *seconds*

Syntax Description	<i>seconds</i> CTS-SXP 再試行タイマー (秒)。範囲は 0 ~ 64000 です。デフォルトは 120 です。
---------------------------	--

Command Default	120 秒 (2 分)
------------------------	-------------

Command Modes	グローバル コンフィギュレーション (config)
----------------------	----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	再試行タイマーは、少なくとも 1 つの CTS-SXP 接続が稼働していない場合にトリガーされます。このタイマーの期限が切れると新しい CTS-SXP 接続が試行されます。ゼロの値は、再試行が発生しなくなります。
-------------------------	--

Related Commands	コマンド	説明
	cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
	cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
	cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
	cts sxp enable	デバイスで CTS-SXP を有効にします。
	cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
	cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
	show cts sxp	CTS-SXP のすべての設定のステータスを表示します。

debug cts environment-data

Cisco TrustSec 環境データ操作のデバッグを有効にするには、特権 EXEC モードで **debug cts environment-data** コマンドを使用します。環境データ操作のデバッグを停止するには、このコマンドの **no** 形式を使用します。

debug cts environment-data [aaa | all | default-epg | default-sg | events | platform | sg-epg]
no debug cts environment-data [aaa | all | default-epg | default-sg | events | platform | sg-epg]

Syntax Description

aaa	(任意) 認証、許可、およびアカウントリング (AAA) メッセージのデバッグを指定します。
all	(任意) すべての環境データメッセージのデバッグを指定します。
default-epg	(任意) デフォルト エンドポイント グループ (EPG) メッセージのデバッグを指定します。
default-sg	(任意) デフォルト サーバグループ メッセージのデバッグを指定します。
events	(任意) 環境データイベントのデバッグを指定します。
platform	(任意) セキュリティグループ タグ (SGT) EPG プラットフォームメッセージのデバッグを指定します。
sg-epg	(任意) SP-EPG マッピングのデバッグを指定します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、環境データイベントのデバッグを有効にする例を示します。

```
Device# enable
Device# debug cts environment-data events
```

Related Commands

コマンド	説明
cts environment-data enable	環境データのダウンロードを有効にします。
clear cts environment-data	環境データをクリアします。
show cts environment-data	Cisco TrustSec の環境データ情報を表示します。

debug cts policy-server

Cisco TrustSec ポリシーサーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug cts policy-server** コマンドを使用します。

```
debug cts policy-server {all | {http | json} {all | error | events}}
```

Syntax Description

all	ポリシーサーバのすべてのデバッグをイネーブルにします。
http	HTTP クライアントのデバッグをイネーブルにします。
json	JSON パーサーのデバッグをイネーブルにします。
error	HTTP エラーのデバッグをイネーブルにします。
events	HTTP イベントのデバッグをイネーブルにします。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、HTTP クライアントエラーのデバッグをイネーブルにする例を示します。

```
Device# enable
Device# debug cts policy-server http error
```

Related Commands

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。
show cts policy-server	Cisco TrustSec ポリシーサーバの情報を表示します。

port (CTS)

ポリシーサーバのポートを設定するには、ポリシーサーバコンフィギュレーションモードで **port** コマンドを使用します。ポリシーサーバのポートを削除するには、このコマンドの **no** 形式を使用します。

```
port port-number
no port
```

Syntax Description	<i>port-number</i>	ポリシーサーバのポート番号。 有効な値は 1025 ~ 65535 です。
---------------------------	--------------------	--

Command Default デフォルトポートは 9063 です。

Command Modes ポリシーサーバ コンフィギュレーション (config-policy-server)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines 外部 RESTful サービス (ERS) ポートとしてサポートされるのは 9063 のみです。

Examples

次に、ポリシーサーバのポートを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# port 9063
```

Related Commands	コマンド	説明
	cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。

propagate sgt (cts manual)

Cisco TrustSec Security (CTS) インターフェイスでレイヤ2のセキュリティグループタグ (SGT) 伝達を有効にするには、インターフェイス コンフィギュレーション モードで **propagate sgt** コマンドを使用します。SGT 伝達を無効にするには、このコマンドの **no** 形式を使用します。

propagate sgt

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

SGT 処理の伝達が有効になっています。

Command Modes

CTS 手動インターフェイス コンフィギュレーション モード (config-if-cts-manual)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

SGT 処理の伝達によって、CTS 対応のインターフェイスは L2 SGT タグに基づいて CTS メタ データ (CMD) を受信および送信できます。ピアデバイスが SGT を受信できず、その結果、SGT タグを L2 ヘッダーに配置できない状況で、インターフェイスの SGT 伝達を無効にするには **no propagate sgt** コマンドを使用します。

Examples

次に、手動で設定された TrustSec 対応のインターフェイスで SGT 伝達を無効にする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# no propagate sgt
```

次に、ギガビットイーサネットインターフェイス0でSGT伝達が無効になっている例を示します。

```
Device#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
  CTS is enabled, mode:      MANUAL
  IFC state:                 OPEN
  Authentication Status:    NOT APPLICABLE
    Peer identity:          "unknown"
    Peer's advertised capabilities: ""
  Authorization Status:    NOT APPLICABLE
  SAP Status:               NOT APPLICABLE
  Propagate SGT:           Disabled
  Cache Info:
    Cache applied to link : NONE
```

Related Commands

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
show cts interface	インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

retransmit (CTS)

サーバからの最大リトライ回数を設定するには、ポリシーサーバコンフィギュレーションモードで **retransmit** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

retransmit *number-of-retries*
no retransmit

Syntax Description	<i>number-of-retries</i>	リトライの最大数。有効な値は 0～5 です。
Command Default	デフォルトは 4 です。	
Command Modes	ポリシーサーバ コンフィギュレーション (config-policy-server)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、最大リトライ回数を変更する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# retransmit 3
```

Related Commands	コマンド	説明
	cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。

sap mode-list (cts manual)

2個のインターフェイスの間のリンク暗号化をネゴシエートするために使用される Security Association Protocol (SAP) の認証と暗号化モード（最高から最低に優先順位付けされた）を選択するには、CTS dot1x インターフェイス コンフィギュレーション モードで **sap mode-list** コマンドを使用します。モードリストを削除してデフォルトに戻すには、このコマンドの **no** 形式を使用します。

2個のインターフェイス間で MACsec のリンク暗号化をネゴシエートするために、ペアワイズマスターキー (PMK) と Security Association Protocol (SAP) の認証および暗号化モードを手動で指定するには、**sap mode-list** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

```
sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]
no sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]
```

Syntax Description

pmk <i>hex_value</i>	16 進数データ PMK を指定します（先行する 0x なし。偶数の 16 進数文字を入力する。そうでない場合は、最後の文字に 0 のプレフィックスが付加される）。
mode-list	アドバタイズされたモードのリストを指定します（最高から最低に優先順位付け）。
gcm-encrypt	GMAC 認証、GCM 暗号化を指定します。
gmac	GMAC 認証だけを指定し、暗号化を指定しません。
no-encap	カプセル化を指定しません。
null	カプセル化あり、認証なし、暗号化なしを指定します。

Command Default

デフォルトのカプセル化は **sap pmk mode-list gcm-encrypt null** です。ピア インターフェイスが 802.1AE MACsec または 802.REV レイヤ 2 リンク暗号化をサポートしない場合、デフォルトの暗号化は **null** です。

Command Modes

CTS 手動インターフェイス コンフィギュレーション (config-if-cts-manual)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

認証と暗号化方式を指定するには、**sap pmk mode-list** コマンドを使用します。

セキュリティ アソシエーション プロトコル (SAP) は 802.11i IEEE プロトコルのドラフトバージョンに基づいた暗号キーの取得および交換プロトコルです。SAP は MACsec をサポートするインターフェイス間の 802.1AE リンク間暗号化 (MACsec) を確立および管理するために使用します。

SAP およびペアワイズマスターキー (PMK) は、**sap pmk mode-list** コマンドを使用して、2 個のインターフェイス間に手動で設定することもできます。802.1X 認証を使用する場合、両方 (サブリカントおよびオーセンティケータ) が Cisco Secure Access Control Server からピアのポートの PMK および MAC アドレスを受信します。

デバイスが CTS 対応ソフトウェアを実行していて、ハードウェアが CTS 非対応である場合は、**sap mode-list no-encap** コマンドを使用してカプセル化を拒否します。

Examples

次に、ギガビットイーサネットインターフェイスで SAP を設定する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 2/1
DeviceD(config-if)# cts manual
Device(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

Related Commands

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
propagate sgt (cts manual)	Cisco TrustSec Security (CTS) インターフェイスのレイヤ 2 でのセキュリティ グループ タグ (SGT) の伝達を有効にします。
show cts interface	Cisco TrustSec インターフェイス設定の統計情報を表示します。

show cts credentials

Cisco TrustSec (CTS) デバイス ID を表示するには、EXEC モードまたは特権 EXEC モードで **show cts credentials** コマンドを使用します。

show cts credentials

Syntax Description このコマンドには、コマンドまたはキーワードはありません。

Command Modes 特権 EXEC (#) ユーザ EXEC (>)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、出力例を示します。

```
Device# show cts credentials
```

```
CTS password is defined in keystore, device-id = r4
```

Related Commands

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。

show cts environment-data

Cisco TrustSec の環境データ情報を表示するには、特権 EXEC モードで **show cts environment-data** コマンドを使用します。

show cts environment-data

このコマンドには、引数およびキーワードはありません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、**show cts environment-data** コマンドの出力例を示します。

```
Device# enable
Device# show cts environment-data

TS Environment Data
=====
Current state = START
Last status = Failed
Environment data is empty
State Machine is running
Retry_timer (60 secs) is running
```

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
cts environment-data enable	環境データのダウンロードを有効にします。
clear cts environment-data	環境データをクリアします。
debug cts environment-data	Cisco TrustSec 環境データ操作のデバッグを有効にします。

show cts interface

インターフェイスの Cisco TrustSec (CTS) 設定の統計を表示するには、EXEC モードまたは特権 EXEC モードで **show cts interface** コマンドを使用します。

show cts interface [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

Syntax Description

<i>port</i>	(任意) ギガビットイーサネットインターフェイス番号。このインターフェイスの冗長ステータス出力が返されます。
<i>number</i>	(任意) VLAN インターフェイス番号 (1 ~ 4095)。
brief	(任意) すべての CTS インターフェイスの短縮ステータスを表示します。
summary	(任意) インターフェイスごとに、すべての CTS インターフェイスのサマリーを、4 個または 5 個のキー ステータス フィールドを持つ表形式で表示します。

Command Default

なし

Command Modes

EXEC (>) 特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

すべての CTS インターフェイスの冗長ステータスを表示するには、キーワードを使用せずに **show cts interface** コマンドを使用します。

Examples

次に、キーワードを使用せずに出力を表示する例を示します (すべての CTS インターフェイスの冗長ステータス)。

```
Device# show cts interface

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:18.232
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Configured pairwise ciphers:
    gcm-encrypt
    null

  Replay protection:      enabled
```

```

Replay protection mode: STRICT

Selected cipher:

Propagate SGT:          Enabled
Cache Info:
  Cache applied to link : NONE

Statistics:
  authc success:        0
  authc reject:         0
  authc failure:        0
  authc no response:    0
  authc logoff:         0
  sap success:          0
  sap fail:             0
  authz success:        0
  authz fail:           0
  port auth fail:      0
Ingress:
  control frame bypassed: 0
  sap frame bypassed:    0
  esp packets:          0
  unknown sa:           0
  invalid sa:           0
  inverse binding failed: 0
  auth failed:          0
  replay error:         0
Egress:
  control frame bypassed: 0
  esp packets:          0
  sgt filtered:         0
  sap frame bypassed:    0
  unknown sa dropped:    0
  unknown sa bypassed:   0

```

次に、**brief** キーワードを使用した出力例を示します。

```

Device# show cts interface brief

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:40.386
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Propagate SGT:          Enabled
  Cache Info:
    Cache applied to link : NONE

```

Related Commands

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
cts sxp enable	ネットワーク デバイスに SXP を設定します。

コマンド	説明
propagate sgt	Cisco TrustSec Security (CTS) インターフェイスのレイヤ 2 でのセキュリティグループタグ (SGT) の伝達を有効にします。

show cts policy-server

Cisco TrustSec ポリシーサーバの情報を表示するには、特権 EXEC モードで **show cts policy-server** コマンドを使用します。

```
show cts policy-server {details | statistics} {active | all name}
```

Syntax Description		
	details	ポリシーサーバの詳細を表示します。
	statistics	ポリシーサーバの統計を表示します。
	active	アクティブなポリシーサーバに関する情報を表示します。
	all	すべてのサーバに関する統計情報を表示します。
	<i>name</i>	ポリシーサーバ名。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、**show cts policy-server details all** コマンドの出力例を示します。

```
Device# enable
Device# show cts policy-server details all

Server Name      : ise_151
Server Status    : Inactive
  IPv4 Address    : 10.1.1.1
  IPv4 Address    : 10.2.2.2
  IPv4 Address    : 10.2.2.3
  IPv6 Address    : 2001:db8::1
  IPv6 Address    : 2001:db8::3
  Domain-name     : www.cisco.ise.com
  Trustpoint      : trust_ise_151
  Port-num        : 9063
  Retransmit count : 3
  Timeout         : 15
  App Content type : JSON

Server Name      : ise_150
Server Status    : Inactive
  IPv4 Address    : 10.64.69.151
  Trustpoint      : trust_ise_151
  Port-num        : 9063
  Retransmit count : 3
```

```
Timeout          : 15
App Content type : JSON
```

次に、**show cts policy-server statistics all** コマンドの出力例を示します。

```
Device# show cts policy-server statistics all
```

```
Server Name   : ise_server_1
Server State  : ALIVE
Number of Request sent      : 7
Number of Request sent fail : 0
Number of Response received : 4
Number of Response rcv fail : 3
  HTTP 200 OK                : 4
  HTTP 400 BadReq            : 0
  HTTP 401 Unauthorized Req  : 0
  HTTP 403 Req Forbidden    : 0
  HTTP 404 NotFound         : 0
  HTTP 408 ReqTimeout       : 0
  HTTP 415 Unsupported Media : 0
  HTTP 500 ServerErr        : 0
  HTTP 501 Req NoSupport    : 0
  HTTP 503 Service Unavailable: 0
TCP or TLS handshake error  : 3
HTTP Other Error           : 0
```

次に、**show cts policy-server statistics name** コマンドの出力例を示します。

```
Device# show cts policy-server statistics name ise_server_1
```

```
Server Name   : ise_server_1
Server State  : ALIVE
Number of Request sent      : 7
Number of Request sent fail : 0
Number of Response received : 4
Number of Response rcv fail : 3
  HTTP 200 OK                : 4
  HTTP 400 BadReq            : 0
  HTTP 401 Unauthorized Req  : 0
  HTTP 403 Req Forbidden    : 0
  HTTP 404 NotFound         : 0
  HTTP 408 ReqTimeout       : 0
  HTTP 415 Unsupported Media : 0
  HTTP 500 ServerErr        : 0
  HTTP 501 Req NoSupport    : 0
  HTTP 503 Service Unavailable: 0
TCP or TLS handshake error  : 3
HTTP Other Error           : 0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 6: show cts policy-server statistics のフィールドの説明

フィールド	説明
HTTP 200 OK	クライアント要求が正常に受け入れられました。

フィールド	説明
HTTP 400 BadReq	要求の形式が正しくないか、要求に無効なパラメータが含まれています。
HTTP 401 Unauthorized Req	リソースにアクセスするための適切なログイン情報（ユーザ名とパスワード）が指定されていません。
HTTP 403 Req Forbidden	クライアント要求がサーバから拒否されました。
HTTP 404 NotFound	URL が無効です。
HTTP 408 ReqTimeout	要求がタイムアウトしました。
HTTP 415 Unsupported Media	サーバで処理できないコンテンツタイプが要求されました。
HTTP 500 ServerErr	内部サーバエラーまたは例外が発生しました。
TCP or TLS handshake error	無効なトラストポイントが原因で、IP に到達できないか Transport Layer Security (TLS) ハンドシェイクに失敗しました。

Related Commands

コマンド	説明
cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバコンフィギュレーションモードを開始します。
debug cts policy-server	Cisco TrustSec ポリシーサーバのデバッグをイネーブルにします。

show cts role-based counters

セキュリティグループアクセスコントロールリスト（ACL）の適用の統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts role-based counters** コマンドを使用します。

```
show cts role-based counters [default [ipv4 | ipv6]] [ {from {sgt-number | unknown}[ipv4 | ipv6] | to | {sgt-number | unknown} | [ipv4 | ipv6]} ] [to {sgt-number | unknown} [ipv4 | ipv6]] [ipv4 | ipv6]
```

Syntax Description	default	(任意) デフォルトポリシーカウンタに関する情報を表示します。
	from	(任意) 送信元セキュリティグループに関する情報を表示します。
	ipv4	(任意) IPv4 ネットワークのセキュリティグループに関する情報を表示します。
	ipv6	(任意) IPv6 ネットワークのセキュリティグループに関する情報を表示します。
	to	(任意) 宛先セキュリティグループに関する情報を表示します。
	sgt-number	(任意) セキュリティグループタグ番号。有効な値は0～65533です。
	unknown	(任意) すべての送信元グループに関する情報を表示します。

Command Modes	ユーザ EXEC (>) 特権 EXEC (#)
---------------	-----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Usage Guidelines	すべてまたは任意の範囲の統計情報をリセットするには、 clear cts role-based counters コマンドを使用します。
------------------	---

from キーワードで送信元 SGT を、**to** キーワードで宛先 SGT を指定します。**from** および **to** の両方のキーワードを省略すると、すべての統計情報が表示されます。

default キーワードは、デフォルトのユニキャストのポリシー統計情報を表示します。**ipv4** および **ipv6** のいずれのキーワードも指定しない場合、このコマンドは IPv4 カウンタだけを表示します。

Cisco TrustSec モニタモードでは、許可されたトラフィックのカウンタが SW-Permitt ラベルの下に表示され、拒否されたトラフィックのカウンタが SW-Monitor ラベルの下に表示されます。

例

次に、**show cts role-based counters**

```
Device# show cts role-based counters
```

```
Role-based IPv4 counters
From      To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor  HW-Monitor
12        24      0          0          0           0           0           0
12        77      0          0          5           0           0           0
```

下の表に、ディスプレイ内に表示される重要なフィールドのリストを示します。

Table 7: show cts role-based counters のフィールドの説明

フィールド	説明
From	送信元セキュリティグループ。
To	宛先セキュリティグループ。
SW-Permitt	許可されたトラフィックのカウンタ。
SW-Monitor	拒否されたトラフィックのカウンタ。

Related Commands

コマンド	説明
clear role-basedcounters	SGACL 統計カウンタをリセットします。
cts role-based	IP アドレス、レイヤ 3 インターフェイス、および VRF を SGT にマッピングします。Cisco TrustSec キャッシングと SGACL の適用を有効にします。

show cts role-based permissions

ロールベース（セキュリティグループ）アクセスコントロール権限リストを表示するには、特権 EXEC モードで **show cts role-based permissions** コマンドを使用します。

```
show cts role-based permissions [default [details | ipv4 [details] | ipv6 [details]] | from { {sgt
| unknown } [ipv4 | ipv6 | to { {sgt | unknown} [details | ipv4 [details] | ipv6 [details]]}} | ipv4
| ipv6 | platform | to {sgt | unknown} [ipv4 | ipv6]]
```

Syntax Description

default	（任意）デフォルトの権限リストに関する情報を表示します。
details	（任意）アタッチされたアクセスコントロールリスト（ACL）の詳細を表示します。
ipv4	（任意）IPv4 プロトコルに関する情報を表示します。
ipv6	（任意）IPv6 プロトコルに関する情報を表示します。
from	（任意）送信元グループに関する情報を表示します。
<i>sgt</i>	（任意）セキュリティ グループ タグ。有効値は 2 ～ 65519 です。
to	（任意）宛先グループに関する情報を表示します。
unknown	（任意）不明な送信元グループと宛先グループに関する情報を表示します。
platform	（任意）プラットフォームに関する情報を表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、SGACL 権限マトリックスのコンテンツを表示します。送信元セキュリティグループタグ（SGT）は **from** キーワードを使用して、宛先 SGT は **to** キーワードを使用して指定できます。両方のキーワードを指定すると、単一セルの RBACL が表示されます。列全体は、**to** キーワードを使用した場合にのみ表示されます。行全体は、**from** キーワードを使用した場合にのみ表示されます。権限マトリックス全体は、**from** キーワードと **to** キーワードの両方を省略した場合に表示されます。

コマンド出力は、プライマリ キーの宛先 SGT およびセカンダリ キーの送信元 SGT でソートされます。各セルの SGACL は、設定で定義されているのと同じ順序で、または Cisco Identity Services Engine（ISE）から取得した順序で表示されます。

details キーワードは、**from** キーワードと **to** キーワードの両方を指定することで、単一のセルが選択された場合にのみ表示されます。**details** キーワードが指定されている場合、単一セルの SGACL のアクセス制御エントリが表示されます。

次に、**show role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):
  mon_1
IPv4 Role-based permissions from group 10 to group 11 (configured):
  mon_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Related Commands

コマンド	説明
cts role-based permissions	送信元グループから宛先グループに対する権限を有効にします。
cts role-based monitor	ロールベースのアクセスリストのモニタリングを有効にします。

show cts server-list

Cisco TrustSec シードおよび非シードデバイスで利用可能な HTTP サーバと RADIUS サーバのリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts server-list** コマンドを使用します。

show cts server-list

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes ユーザ EXEC (>
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.1.1	このコマンドの出力が変更され、HTTPサーバのアドレスとステータス情報が表示されるようになりました。
Cisco IOS XE Amsterdam 17.2.1	このコマンドの出力が変更され、HTTPサーバのIPv6アドレスが表示されるようになりました。

Usage Guidelines

このコマンドは、Cisco TrustSec RADIUS サーバのアドレスとステータス情報を収集するのに使用できます。

Cisco IOS XE Gibraltar 17.1.1 以降のリリースでは、このコマンドの出力に HTTP サーバのアドレスとステータス情報が表示されます。

Cisco IOS XE Gibraltar 17.2.1 以降のリリースでは、このコマンドの出力に HTTP サーバの IPv4 アドレスと共に IPv6 アドレスが表示されます。

Examples

Cisco IOS XE Amsterdam 17.2.1 以降のリリース

次の **show cts server-list** コマンドの出力例では、HTTP サーバの IPv4 アドレスおよび IPv6 アドレスとそのステータス情報が表示されています。

```
Device> show cts server-list

HTTP Server-list:
  Server Name   : cts_private_server_0
  Server State  : ALIVE
  IPv4 Address  : 10.64.69.151
  IPv6 Address  : 2001:DB8:8086:6502::
  IPv6 Address  : 2001:db8::2
  IPv6 Address  : 2001:db8::402:99
  IPv6 Address  : 2001:DB8::802:16
  Domain-name   : ise-267.cisco.com
  Trustpoint    : cts_trustpoint_0
```

```

Server Name   : cts_private_server_1
Server State  : ALIVE
IPv4 Address  : 10.10.10.3
IPv4 Address  : 10.10.10.2
IPv6 Address  : 2001:db8::20
IPv6 Address  : 2001:db8::21
Domain-name   : www.ise.cisco.com
Trustpoint    : cts_trustpoint_1

```

Cisco IOS XE Amsterdam 17.1.1

次の **show cts server-list** コマンドの出力例では、HTTP サーバとそのステータス情報が表示されています。

```

Device> show cts server-list

HTTP Server-list:
Server Name: Http_Server_1
Server Status: DEAD
    IPv4 Address: 10.78.105.148
    IPv6 Address: Not Supported
    Domain-name: http_server_1.ise.com
    Port: 9063

Server Name: Http_Server_2
Server Status: ALIVE
    IPv4 Address: 10.78.105.149
    IPv6 Address: Not Supported
    Domain-name: http_server_2.ise.com
    Status = ALIVE

```

Cisco IOS XE Amsterdam 17.1.1 より前のリリース

次の例では、Cisco TrustSec RADIUS サーバのリストが表示されています。

```

Device> show cts server-list

CTS Server Radius Load Balance = DISABLED
Server Group Deadtme = 20 secs (default)
Global Server Liveness Automated Test Deadtme = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)
Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
    Status = ALIVE
    auto-test = TRUE, idle-time = 60 mins, deadtme = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
    Status = ALIVE
    auto-test = TRUE, idle-time = 60 mins, deadtme = 20 secs

```

Related Commands

コマンド	説明
address ipv4 (config-radius-server)	PAC プロビジョニングに使用する RADIUS サーバのアカウントニングおよび認証パラメータを設定します。

コマンド	説明
pac key	PAC 暗号キーを指定します。

show cts sxp

Cisco TrustSec セキュリティグループタグ (SGT) 交換プロトコル (CTS-SXP) 接続または送信元 IP と SGT のマッピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts sxp** コマンドを使用します。

```
show cts sxp {connections [brief | vrf instance-name] | filter-group [detailed | global | listener | speaker] | filter-list filter-list-name | sgt-map [brief | vrf instance-name]} [brief | vrf instance-name]
```

Syntax Description		
	connections	Cisco TrustSec SXP 接続の情報を表示します。
	brief	(任意) SXP 情報の省略形を表示します。
	vrf instance-name	(任意) 指定した Virtual Routing and Forwarding (VRF) インスタンスの SXP 情報を表示します。
	filter-group {detailed global listener speaker }	(任意) フィルタグループ情報を表示します。
	filter-list filter-list-name	(任意) フィルタリスト情報を表示します。
	sgt-map	(任意) SXP 経由で受信した IP と SGT のマッピングを表示します。

Command Default なし

Command Modes ユーザ EXEC (>) 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**brief** キーワードを使用して SXP 接続を表示する例を示します。

```
Device# show cts sxp connection brief

SXP                : Enabled
Default Password   : Set
Default Source IP  : Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running

-----
Peer_IP           Source_IP         Conn Status      Duration
-----
10.10.10.1        10.10.10.2       On               0:00:02:14 (dd:hr:mm:sec)
10.10.2.1        10.10.2.2        On               0:00:02:14 (dd:hr:mm:sec)
```

Total num of SXP Connections = 2

次に、CTS-SXP 接続を表示する例を示します。

```
Device# show cts sxp connections

SXP                : Enabled
Default Password   : Set
Default Source IP  : Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
Peer IP            : 10.10.10.1
Source IP          : 10.10.10.2
Set up             : Peer
Conn status        : On
Connection mode    : SXP Listener
Connection inst#   : 1
TCP conn fd        : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
-----
Peer IP            : 10.10.2.1
Source IP          : 10.10.2.2
Set up             : Peer
Conn status        : On
Connection mode    : SXP Listener
TCP conn fd        : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

次に、デバイスがスピーカーとリスナーの両方である場合に双方向接続の CTS-SXP 接続を表示する例を示します。

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
-----
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

次に、SXPスピーカーへの接続が切断されたCTS-SXPリスナーからの出力例を示します。送信元 IP と SGT のマッピングは 120 秒（削除のホールドダウンタイマーのデフォルト値）の間保持されます。

```
Device# show cts sxp connections

SXP                : Enabled
Default Password   : Set
Default Source IP  : Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
Peer IP            : 10.10.10.1
Source IP          : 10.10.10.2
Set up             : Peer
Conn status        : Delete_Hold_Down
Connection mode    : SXP Listener
Connection inst#   : 1
TCP conn fd        : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
-----
Peer IP            : 10.10.2.1
Source IP          : 10.10.2.2
Set up             : Peer
Conn status        : On
Connection inst#   : 1
TCP conn fd        : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

Related Commands

コマンド	説明
cts sxp connection peer	Cisco TrustSec SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	Cisco TrustSec SXP のデフォルトパスワードを設定します。
cts sxp default source-ip	Cisco TrustSec SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで Cisco TrustSec SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	Cisco TrustSec SXP の復帰期間を変更します。
cts sxp retry	Cisco TrustSec SXP の再試行期間タイマーを変更します。

show platform hardware fed switch active fwd-asic resource tcam utilization

ASIC の CAM 使用率情報を表示するには、特権 EXEC モードで **show platform hardware fed switch active fwd-asic resource tcam utilization** コマンドを使用します。

show platform hardware fed switch active fwd-asic resource tcam utilization [*asic-number*] [*slice-id*]

Syntax Description	asic-number	ASIC 番号を表示します。有効な値の範囲は 0 ~ 7 です。
---------------------------	--------------------	----------------------------------

	slice-id	スライスごとの使用状況を表示します。
--	-----------------	--------------------

Command Modes	特権 EXEC (#)
----------------------	-------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Examples

次に、**show platform hardware fed switch active fwd-asic resource tcam utilization** コマンドの出力例を示します。

```
Device# enable
Device# show platform hardware fed switch active fwd-asic resource tcam utilization

CAM Utilization for ASIC [0]
Table          Subtype      Dir      Max      Used      %Used      V4      V6
MPLS          Other
-----
Mac Address Table      EM          I        32768    25        0.08%      0        0
  0          25
Mac Address Table      TCAM       I         1024    22         2.15%      0        0
  0          22
L3 Multicast          EM          I         8192     0         0.00%      0        0
  0          0
L3 Multicast          TCAM       I          512     9         1.76%      3        6
  0          0
L2 Multicast          EM          I         8192     0         0.00%      0        0
  0          0
L2 Multicast          TCAM       I          512    11         2.15%      3        8
  0          0
IP Route Table        EM          I       24576    14         0.06%     13        0
  1          0
IP Route Table        TCAM       I         8192    30         0.37%     11       16
  2          1
QOS ACL               TCAM       IO        5120    85         1.66%     28       38
  0          19
                   TCAM       I          45         0.88%     15       20
  0          10
```

0	9	TCAM	O		40	0.78%	13	18
Security ACL		TCAM	IO	5120	131	2.56%	26	60
0	45	TCAM	I		88	1.72%	12	36
0	40	TCAM	O		43	0.84%	14	24
0	5	TCAM	I	256	6	2.34%	2	2
Netflow ACL		TCAM	I	1024	36	3.52%	30	6
0	2	TCAM	O	768	6	0.78%	2	2
PBR ACL		TCAM	IO	1024	13	1.27%	3	6
0	0	TCAM	I		5	0.49%	1	2
Netflow ACL		TCAM	O		8	0.78%	2	4
0	2	TCAM	I	512	290	56.64%	138	106
Control Plane		TCAM	I	512	22	4.30%	9	13
0	46	TCAM	I	2048	2	0.10%	0	0
Tunnel Termination		TCAM	I	256	4	1.56%	2	2
0	0	EM	O	8192	0	0.00%	0	0
Lisp Inst Mapping		TCAM	O	512	1	0.20%	0	0
0	2	EM	I	4096	0	0.00%	0	0
Security Association		TCAM	I	256	0	0.00%	0	0
0	0	TCAM	O	1024	0	0.00%	0	0
CTS Cell Matrix/VPN Label		TCAM	O	1024	0	0.00%	0	0
0	0	TCAM	I	256	2	0.78%	0	0
CTS Cell Matrix/VPN Label		TCAM	I	256	2	0.78%	0	0
0	1	EM	I	4096	0	0.00%	0	0
Client Table		TCAM	I	256	0	0.00%	0	0
0	0	TCAM	I	1024	0	0.00%	0	0
Client Table		TCAM	O	1024	0	0.00%	0	0
0	0	TCAM	O	1024	0	0.00%	0	0
Input Group LE		TCAM	O	1024	0	0.00%	0	0
0	0	TCAM	O	1024	0	0.00%	0	0
Output Group LE		TCAM	O	1024	0	0.00%	0	0
0	0	TCAM	O	1024	0	0.00%	0	0
Macsec SPD		TCAM	I	256	2	0.78%	0	0
0	2	TCAM	I	256	2	0.78%	0	0

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
show platform hardware fed switch active fwd-asic resource tcam table	現在の CAM テーブルを表示します。
show platform hardware fed switch active fwd-asic resource tcam usage	現在の CAM の使用状況を表示します。

show platform hardware fed switch active sgACL resource usage

特定用途向け集積回路（ASIC）のセキュリティグループアクセスコントロールリスト（SGACL）のリソース情報を表示するには、特権 EXEC モードで **show platform hardware fed switch active sgACL resource usage** コマンドを使用します。

show platform hardware fed switch active sgACL resource usage

Syntax Description	usage	SGACL リソースの使用状況を表示します。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Examples

次に、**show platform hardware fed switch active sgACL resource usage** コマンドの出力例を示します。

```
Device# enable
Device# show platform hardware fed switch active sgACL resource usage

SGACL RESOURCE DETAILS ASIC :#0
=====
Hardware Resource           MAX      Used      Percent
                               Used      Used      Used
                               -----
CTS Cell Matrix Config      :          :          :
CTS Cell Matrix Entries     : 8192    0          0
CTS Cell Overflow Entries   :  512    1          0

Policy Configuration        :          :          :
Policy Entries               :  256    3          1

DGT Config                   :          :          :
DGT Entries                  : 4096    0          0

Security ACL Configured     :          :          :
Security ACL Entries        : 5120    131        2

                               Total      Percent
                               Used      Used
-----
Output PRE SGACL            :         4      12
Output SGACL                 :         0       0
Output SGACL DEFAULT        :         0       0
.
.
.
Device#
```

出力フィールドの意味は自明です。

show platform software classification switch active F0 class-group-manager class-group client acl all

Ternary Content Addressable Memory (TCAM) エントリの表示に使用される ACL クラスグループ ID を表示するには、特権 EXEC モードで **show platform software classification switch active F0 class-group-manager class-group client acl all** コマンドを使用します。

show platform software classification switch active F0 class-group-manager class-group client acl all

Syntax Description	class-group-manager	クラスグループマネージャを表示します。
	class-group	クラスグループを表示します。
	all	すべてのクラスグループの ACL クラスグループ ID を表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software classification switch active F0 class-group-manager class-group client acl all** コマンドの出力例を示します。

```
Device#show platform software classification switch active F0 class-group-manager class-group client acl all
```

```
QFP classification class client all group
```

```
class-group [ACL-GRP:273]
class-group [ACL-GRP:529]
class-group [ACL-GRP:801]
```

出力フィールドの意味は自明です。

Related Commands	コマンド	説明
	show platform software classification switch active F0 class-group-manager class-group client acl name <i>class-group name</i>	指定されたクラスグループの ACL クラスグループ情報を表示します。
	show platform software classification switch active F0 class-group-manager class-group client acl <i>class-group id</i>	指定されたクラスグループの ACL クラスグループ情報を表示します。

show platform software cts forwarding-manager switch active F0 port

転送マネージャインターフェイスのCTS情報を表示するには、特権EXECモードで **show platform software cts forwarding-manager switch active F0 port** コマンドを使用します。

show platform software cts forwarding-manager switch active F0 port

Syntax Description	F0 Embedded Service Processor スロット 0。
	port ポートCTSステータスを表示します。
Command Modes	特権 EXEC (#)
Command History	リリース Cisco IOS XE Fuji 16.9.1 変更内容 このコマンドが導入されました。

例

次に、**show platform software cts forwarding-manager switch active F0 port** コマンドの出力例を示します。

```
Device#show platform software cts forwarding-manager switch active F0 port
```

```
Forwarding Manager Interfaces CTS Information
```

Name	ID	CTS Enable	Trusted	Propagate	SGT value
GigabitEthernet1/0/1	77	0	0	0	0
GigabitEthernet1/0/3	79	0	0	0	0
GigabitEthernet1/0/4	80	0	0	0	0
GigabitEthernet1/0/5	81	0	0	0	0
GigabitEthernet1/0/6	82	0	0	0	0
GigabitEthernet1/0/7	83	0	0	0	0
GigabitEthernet1/0/8	84	0	0	0	0
GigabitEthernet1/0/9	85	0	0	0	0
GigabitEthernet1/0/10	86	0	0	0	0
GigabitEthernet1/0/11	87	0	0	0	0
GigabitEthernet1/0/12	88	0	0	0	0
GigabitEthernet1/0/13	89	0	0	0	0
GigabitEthernet1/0/14	90	0	0	0	0
GigabitEthernet1/0/15	91	0	0	0	0
GigabitEthernet1/0/16	92	0	0	0	0
GigabitEthernet1/0/17	93	0	0	0	0
GigabitEthernet1/0/18	94	0	0	0	0
GigabitEthernet1/0/19	95	0	0	0	0
GigabitEthernet1/0/20	96	0	0	0	0
GigabitEthernet1/0/21	97	0	0	0	0
GigabitEthernet1/0/22	98	0	0	0	0
GigabitEthernet1/0/23	99	0	0	0	0
GigabitEthernet1/0/24	100	0	0	0	0
GigabitEthernet1/0/25	101	0	0	0	0

GigabitEthernet1/0/26	102	0	0	0	0
GigabitEthernet1/0/27	103	0	0	0	0
GigabitEthernet1/0/28	104	0	0	0	0
GigabitEthernet1/0/29	105	0	0	0	0
GigabitEthernet1/0/30	106	0	0	0	0
GigabitEthernet1/0/31	107	0	0	0	0
GigabitEthernet1/0/32	108	0	0	0	0
GigabitEthernet1/0/33	109	0	0	0	0
GigabitEthernet1/0/34	110	0	0	0	0
GigabitEthernet1/0/35	111	0	0	0	0
GigabitEthernet1/0/36	112	0	0	0	0
GigabitEthernet1/0/37	113	0	0	0	0
GigabitEthernet1/0/38	114	0	0	0	0
GigabitEthernet1/0/39	115	0	0	0	0
GigabitEthernet1/0/40	116	0	0	0	0
GigabitEthernet1/0/41	117	0	0	0	0

Forwarding Manager Interfaces CTS Information

Name	ID	CTS Enable	Trusted	Propagate	SGT value
GigabitEthernet1/0/42	118	0	0	0	0
GigabitEthernet1/0/43	119	0	0	0	0
GigabitEthernet1/0/44	120	0	0	0	0
GigabitEthernet1/0/45	121	0	0	0	0
GigabitEthernet1/0/46	122	0	0	0	0
GigabitEthernet1/0/47	123	0	0	0	0
GigabitEthernet1/1/1	125	0	0	0	0
GigabitEthernet1/1/2	126	0	0	0	0
GigabitEthernet1/1/3	127	0	0	0	0
GigabitEthernet1/1/4	128	0	0	0	0
TenGigabitEthernet1/1/1	129	0	0	0	0
TenGigabitEthernet1/1/2	130	0	0	0	0
TenGigabitEthernet1/1/3	131	0	0	0	0
TenGigabitEthernet1/1/4	132	0	0	0	0
TenGigabitEthernet1/1/5	133	0	0	0	0
TenGigabitEthernet1/1/6	134	0	0	0	0
TenGigabitEthernet1/1/7	135	0	0	0	0
TenGigabitEthernet1/1/8	136	0	0	0	0
FortyGigabitEthernet1/1/1	137	0	0	0	0
FortyGigabitEthernet1/1/2	138	0	0	0	0
TwentyFiveGigE1/1/1	139	0	0	0	0
TwentyFiveGigE1/1/2	140	0	0	0	0
AppGigabitEthernet1/0/1	141	0	0	0	0
GigabitEthernet2/0/1	142	1	0	0	0
GigabitEthernet2/0/2	143	0	0	0	0
GigabitEthernet2/0/3	144	0	0	0	0
GigabitEthernet2/0/4	145	0	0	0	0
GigabitEthernet2/0/5	146	0	0	0	0
GigabitEthernet2/0/6	147	0	0	0	0
GigabitEthernet2/0/7	148	0	0	0	0
GigabitEthernet2/0/8	149	0	0	0	0
GigabitEthernet2/0/9	150	0	0	0	0
GigabitEthernet2/0/10	151	0	0	0	0
GigabitEthernet2/0/11	152	0	0	0	0
GigabitEthernet2/0/12	153	0	0	0	0
GigabitEthernet2/0/13	154	0	0	0	0
GigabitEthernet2/0/14	155	0	0	0	0
GigabitEthernet2/0/15	156	0	0	0	0
GigabitEthernet2/0/16	157	0	0	0	0
GigabitEthernet2/0/17	158	0	0	0	0

show platform software cts forwarding-manager switch active F0 port

Forwarding Manager Interfaces CTS Information

Name	ID	CTS Enable	Trusted	Propagate	SGT value
GigabitEthernet2/0/18	159	0	0	0	0
GigabitEthernet2/0/19	160	0	0	0	0
GigabitEthernet2/0/20	161	0	0	0	0
GigabitEthernet2/0/21	162	0	0	0	0
GigabitEthernet2/0/22	163	0	0	0	0
GigabitEthernet2/0/23	164	0	0	0	0
GigabitEthernet2/0/24	165	0	0	0	0
GigabitEthernet2/0/25	166	0	0	0	0
GigabitEthernet2/0/26	167	0	0	0	0
GigabitEthernet2/0/27	168	0	0	0	0
GigabitEthernet2/0/28	169	0	0	0	0
GigabitEthernet2/0/29	170	0	0	0	0
GigabitEthernet2/0/30	171	0	0	0	0
GigabitEthernet2/0/31	172	0	0	0	0
GigabitEthernet2/0/32	173	0	0	0	0
GigabitEthernet2/0/33	174	0	0	0	0
GigabitEthernet2/0/34	175	0	0	0	0
GigabitEthernet2/0/35	176	0	0	0	0
GigabitEthernet2/0/36	177	0	0	0	0
GigabitEthernet2/0/37	178	0	0	0	0
GigabitEthernet2/0/38	179	0	0	0	0
GigabitEthernet2/0/39	180	0	0	0	0
GigabitEthernet2/0/40	181	0	0	0	0
GigabitEthernet2/0/41	182	0	0	0	0
GigabitEthernet2/0/42	183	0	0	0	0
GigabitEthernet2/0/43	184	0	0	0	0
GigabitEthernet2/0/44	185	0	0	0	0
GigabitEthernet2/0/45	186	0	0	0	0
GigabitEthernet2/0/46	187	0	0	0	0
GigabitEthernet2/0/47	188	0	0	0	0
GigabitEthernet2/1/1	190	0	0	0	0
GigabitEthernet2/1/2	191	0	0	0	0
GigabitEthernet2/1/3	192	0	0	0	0
GigabitEthernet2/1/4	193	0	0	0	0
TenGigabitEthernet2/1/1	194	0	0	0	0
TenGigabitEthernet2/1/2	195	0	0	0	0
TenGigabitEthernet2/1/3	196	0	0	0	0
TenGigabitEthernet2/1/4	197	0	0	0	0
TenGigabitEthernet2/1/5	198	0	0	0	0
TenGigabitEthernet2/1/6	199	0	0	0	0

Forwarding Manager Interfaces CTS Information

Name	ID	CTS Enable	Trusted	Propagate	SGT value
TenGigabitEthernet2/1/7	200	0	0	0	0
TenGigabitEthernet2/1/8	201	0	0	0	0
FortyGigabitEthernet2/1/1	202	0	0	0	0
FortyGigabitEthernet2/1/2	203	0	0	0	0
TwentyFiveGigE2/1/1	204	0	0	0	0
TwentyFiveGigE2/1/2	205	0	0	0	0
AppGigabitEthernet2/0/1	206	0	0	0	0
GigabitEthernet1/0/2	213	0	0	0	0

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 8: show platform software cts forwarding-manager switch active F0 port のフィールドの説明

フィールド	説明
Name	インターフェイスの名前。
ID	インターフェイス ID。
CTS Enable	CTS のステータス。
Trusted	インターフェイスの信頼ステータス。
Propagate	インターフェイスの伝達ステータス。
SGT value	SGT の値。

show platform software cts forwarding-manager switch active F0

セキュリティグループタグ (SGT) バインドテーブルを表示するには、特権 EXEC モードで **show platform software cts forwarding-manager switch active F0** コマンドを使用します。

show platform software cts forwarding-manager switch active F0

Syntax Description	F0 Embedded Service Processor スロット 0 を選択します。				
Command Modes	特権 EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.1</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。				

例

次に、**show platform software cts forwarding-manager switch active F0** コマンドの出力例を示します。

```
Device#show platform software cts forwarding-manager switch active F0
SGT Binding Table
Number of bindings: 1
2.2.2.2/32
SGT Src: 2
SGT Dst: 2
```

SGT Binding Table

出力フィールドの意味は自明です。

Related Commands	コマンド	説明
	show platform software cts forwarding-manager switch active F0 port	ポート CTS ステータスを表示します。
	show platform software cts forwarding-manager switch active F0 permissions	SGACL 権限を表示します。

show platform software cts forwarding-manager switch active F0 permissions

セキュリティ グループ アクセス コントロール リスト (SGACL) の権限を表示するには、特権 EXEC モードで **show platform software cts forwarding-manager switch active F0 permissions** コマンドを使用します。

show platform software cts forwarding-manager switch active F0 permissions

Syntax Description

F0 Embedded Service Processor スロット 0 を選択します。

permissions SGACL 権限を表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software cts forwarding-manager switch active F0 permissions** コマンドの出力例を示します。

```
Device#show platform software cts forwarding-manager switch active F0 permissions
```

```
Forwarding Manager CTS permissions Information
```

```
  sgt      dgt      ACL Group Name
```

```
  4        2        V4SGACL7100
```

```
65535    65535    V4SGACL8100
```

```
65535    65535    V6SGACL9100
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 9: show platform software cts forwarding-manager switch active F0 permissions のフィールドの説明

フィールド	説明
sgt	送信元グループタグ。

dgt	接続先グループタグ。
ACL Group Name	ACL グループの名前。

show platform software fed switch active acl counters hardware | inc SGACL

フォワーディング エンジン ドライバからのカウンタを表示するには、特権 EXEC モードで **show platform software fed switch active acl counters hardware | inc SGACL** コマンドを使用します。

show platform software fed switch active acl counters hardware | inc SGACL

Syntax Description

counters	カウンタ情報を表示します。
hardware	ハードウェアカウンタを表示します。
include	指定された文字列に一致する行を含めます。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active acl counters hardware | inc SGACL** コマンドの出力例を示します。

```
Device# show platform software fed switch active acl counters hardware | inc SGACL

Egress IPv4 SGACL Drop          (0x3f000061):          0 frames
Egress IPv6 SGACL Drop          (0x13000062):          0 frames
Egress IPv4 SGACL Test Cell Drop (0xd2000063):          0 frames
Egress IPv6 SGACL Test Cell Drop (0x40000064):          0 frames
Egress IPv4 Pre SGACL Forward   (0x2c000067):          0 frames
```

show platform software fed switch active acl usage

セキュリティグループアクセスコントロールリスト（SGACL）の使用状況を表示するには、特権 EXEC モードで **show platform software fed switch active acl usage** コマンドを使用します。

show platform software fed switch active acl usage

Syntax Description

usage ACLの使用状況を表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active acl usage** コマンドの出力例を示します。

```
Device# show platform software fed switch active acl usage
#####
#####
#####      Printing Usage Infos      #####
#####
#####
##### ACE Software VMR max:196608 used:282
#####
```

```
=====
Feature Type      ACL Type      Dir      Name      Entries
Used
SGACL             IPV4          Egress   V4SGACL7100      2
```

```
=====
Feature Type      ACL Type      Dir      Name      Entries
Used
SGACL_CATCHALL   IPV4          Egress   V4SGACL8100      1
```

```
=====
Feature Type      ACL Type      Dir      Name      Entries
Used
SGACL_CATCHALL   IPV6          Egress   V6SGACL9100      1
=====
```

出力フィールドの意味は自明です。

show platform software fed switch active ifm mappings

show platform software fed switch active ifm mappings

Syntax Description	ifm インターフェイスマネージャ情報を表示します。
	mappings インターフェイスからハードウェアへのマッピング情報を表示します。
Command Modes	特権 EXEC (#)
Command History	リリース 変更内容
	Cisco IOS XE Fuji 16.9.1 このコマンドが導入されました。

例

次に、**show platform software fed switch active ifm mappings** コマンドの出力例を示します。

```
Device#show platform software fed switch active ifm mappings
```

Interface	IF_ID	Inst	Asic	Core	Port	SubPort	Mac	Cntx	LPN	GPN	Type
Active											
GigabitEthernet3/0/1	0xa	1	0	1	0	0	26	6	1	193	NIF Y
GigabitEthernet3/0/2	0xb	1	0	1	1	0	6	7	2	194	NIF Y
GigabitEthernet3/0/3	0xc	1	0	1	2	0	28	8	3	195	NIF Y
GigabitEthernet3/0/4	0xd	1	0	1	3	0	27	9	4	196	NIF Y
GigabitEthernet3/0/5	0xe	1	0	1	4	0	30	10	5	197	NIF Y
GigabitEthernet3/0/6	0xf	1	0	1	5	0	29	11	6	198	NIF Y
GigabitEthernet3/0/7	0x10	1	0	1	6	0	32	12	7	199	NIF Y
GigabitEthernet3/0/8	0x11	1	0	1	7	0	31	13	8	200	NIF Y
GigabitEthernet3/0/9	0x12	1	0	1	8	0	19	14	9	201	NIF Y
GigabitEthernet3/0/10	0x13	1	0	1	9	0	5	15	10	202	NIF Y
GigabitEthernet3/0/11	0x14	1	0	1	10	0	21	16	11	203	NIF Y
GigabitEthernet3/0/12	0x15	1	0	1	11	0	20	17	12	204	NIF Y
GigabitEthernet3/0/13	0x16	1	0	1	12	0	23	18	13	205	NIF Y
GigabitEthernet3/0/14	0x17	1	0	1	13	0	22	19	14	206	NIF Y
GigabitEthernet3/0/15	0x18	1	0	1	14	0	25	20	15	207	NIF Y
GigabitEthernet3/0/16	0x19	1	0	1	15	0	24	21	16	208	NIF Y
GigabitEthernet3/0/17	0x1a	1	0	1	16	0	12	22	17	209	NIF Y
GigabitEthernet3/0/18	0x1b	1	0	1	17	0	4	23	18	210	NIF Y
GigabitEthernet3/0/19	0x1c	1	0	1	18	0	14	24	19	211	NIF Y
GigabitEthernet3/0/20	0x1d	1	0	1	19	0	13	25	20	212	NIF Y
GigabitEthernet3/0/21	0x1e	1	0	1	20	0	16	26	21	213	NIF Y
GigabitEthernet3/0/22	0x1f	1	0	1	21	0	15	27	22	214	NIF Y
GigabitEthernet3/0/23	0x20	1	0	1	22	0	18	28	23	215	NIF Y
GigabitEthernet3/0/24	0x21	1	0	1	23	0	17	29	24	216	NIF Y
GigabitEthernet3/0/25	0x22	0	0	0	24	0	26	6	25	217	NIF Y
GigabitEthernet3/0/26	0x23	0	0	0	25	0	6	7	26	218	NIF Y
GigabitEthernet3/0/27	0x24	0	0	0	26	0	28	8	27	219	NIF Y
GigabitEthernet3/0/28	0x25	0	0	0	27	0	27	9	28	220	NIF Y
GigabitEthernet3/0/29	0x26	0	0	0	28	0	30	10	29	221	NIF Y
GigabitEthernet3/0/30	0x27	0	0	0	29	0	29	11	30	222	NIF Y
GigabitEthernet3/0/31	0x28	0	0	0	30	0	32	12	31	223	NIF Y
GigabitEthernet3/0/32	0x29	0	0	0	31	0	31	13	32	224	NIF Y
GigabitEthernet3/0/33	0x2a	0	0	0	32	0	19	14	33	225	NIF Y
GigabitEthernet3/0/34	0x2b	0	0	0	33	0	5	15	34	226	NIF Y

show platform software fed switch active ifm mappings

```

GigabitEthernet3/0/35    0x2c    0 0 0    34    0    21 16 35 227 NIF Y
GigabitEthernet3/0/36    0x2d    0 0 0    35    0    20 17 36 228 NIF Y
GigabitEthernet3/0/37    0x2e    0 0 0    36    0    23 18 37 229 NIF Y
GigabitEthernet3/0/38    0x2f    0 0 0    37    0    22 19 38 230 NIF Y
GigabitEthernet3/0/39    0x30    0 0 0    38    0    25 20 39 231 NIF Y
GigabitEthernet3/0/40    0x31    0 0 0    39    0    24 21 40 232 NIF Y
GigabitEthernet3/0/41    0x32    0 0 0    40    0    12 22 41 233 NIF Y
GigabitEthernet3/0/42    0x33    0 0 0    41    0    4 23 42 234 NIF Y
GigabitEthernet3/0/43    0x34    0 0 0    42    0    14 24 43 235 NIF Y
GigabitEthernet3/0/44    0x35    0 0 0    43    0    13 25 44 236 NIF Y
GigabitEthernet3/0/45    0x36    0 0 0    44    0    16 26 45 237 NIF Y
GigabitEthernet3/0/46    0x37    0 0 0    45    0    15 27 46 238 NIF Y
GigabitEthernet3/0/47    0x38    0 0 0    46    0    18 28 47 239 NIF Y
GigabitEthernet3/0/48    0xd8    0 0 0    47    0    17 29 48 240 NIF Y
GigabitEthernet3/1/1     0x3a    1 0 1    48    0    3 4 49 241 NIF N
GigabitEthernet3/1/2     0x3b    1 0 1    49    0    2 5 50 242 NIF N
GigabitEthernet3/1/3     0x3c    0 0 0    50    0    3 4 51 243 NIF N
GigabitEthernet3/1/4     0x3d    0 0 0    51    0    2 5 52 244 NIF N
TenGigabitEthernet3/1/1  0x3e    1 0 1    52    0    3 3 53 245 NIF N
TenGigabitEthernet3/1/2  0x3f    1 0 1    53    0    2 2 54 246 NIF N
TenGigabitEthernet3/1/3  0x40    1 0 1    54    0    1 1 55 247 NIF N
TenGigabitEthernet3/1/4  0x41    1 0 1    55    0    0 0 56 248 NIF N
TenGigabitEthernet3/1/5  0x42    0 0 0    56    0    3 3 57 249 NIF N
TenGigabitEthernet3/1/6  0x43    0 0 0    57    0    2 2 58 250 NIF N
TenGigabitEthernet3/1/7  0x44    0 0 0    58    0    1 1 59 251 NIF N
TenGigabitEthernet3/1/8  0x45    0 0 0    59    0    0 0 60 252 NIF N
FortyGigabitEthernet3/1/1 0x46    1 0 1    60    0    0 0 61 253 NIF N
FortyGigabitEthernet3/1/2 0x47    0 0 0    61    0    0 0 62 254 NIF N
TwentyFiveGigE3/1/1     0x48    1 0 1    62    0    0 0 63 255 NIF N
TwentyFiveGigE3/1/2     0x49    0 0 0    63    0    0 0 64 256 NIF N
AppGigabitEthernet3/0/1  0x4a    1 0 1    24    0    11 30 65 257 NIF Y

```

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 10: show platform software fed switch active ifm mappings のフィールドの説明

フィールド	説明
Interface	インターフェイスの名前。
IF_ID	インターフェイス ID。
Inst	インスタンス ID。
Asic	ASIC 番号。
Core	コア番号。
Port	インターフェイスのポート番号。
SubPort	サブポートの数。
MAC	MAC アドレス。
LPN	ASIC 内のローカルポート番号。
GPN	スイッチ内のグローバルシステム番号。

タイプ	インターフェイスのタイプ。
アクティブ	インターフェイスのステータス（アクティブ/非アクティブ）。

show platform software fed switch active ip route

IP ルート情報を表示するには、特権 EXEC モードで **show platform software fed switch active ip route** コマンドを使用します。

show platform software fed switch active ip route

Syntax Description

ip IP コマンドを受け入れます。

route IPv4 転送情報ベース（FIB）の詳細を表示します。

Command Modes

特権 EXEC（#）

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.1

このコマンドが導入されました。

例

次に、**show platform software fed switch active ip route** コマンドの出力例を示します。

```
Device# show platform software fed switch active ip route
vrf  dest                               htm          flags  SGT  DGID MPLS
  Last-modified           SecsSinceHit
---  ----          ---          -
-----
2      0.0.0.0/0                               0x78f2fd3488a8 0x0    0    0
  2023/03/14 06:38:18.684                1
2      127.0.0.0/8                               0x78f2fd351508 0x0    0    0
  2023/03/14 06:38:18.687                1
2      255.255.255.255/32                       0x78f2fd34ebd8 0x0    0    0
  2023/03/14 06:38:18.686                1
2      240.0.0.0/4                               0x78f2fd350828 0x0    0    0
  2023/03/14 06:38:18.686                1
2      0.0.0.0/32                               0x78f2fd34cd88 0x0    0    0
  2023/03/14 06:38:18.685                1
2      0.0.0.0/8                               0x78f2fd350e98 0x0    0    0
  2023/03/14 06:38:18.686                1
0      0.0.0.0/0                               0x78f2fd345388 0x0    0    0
  2023/03/14 06:39:09.383                352
0      9.24.0.0/32                               0x78f2fd33e1c8 0x0    0    0
  2023/03/14 06:38:38.930                1
0      9.24.0.1/32                               0x78f2fd33a5e8 0x0    0    0
  2023/03/14 06:39:09.390                5
0      127.0.0.0/8                               0x78f2fd3501b8 0x0    0    0
  2023/03/14 06:38:18.686                1
0      255.255.255.255/32                       0x78f2fd34c478 0x0    0    0
  2023/03/14 06:38:18.685                1
0      2.2.2.2/32                               0x78f2fd3568e8 0x0    2    1
  2023/03/14 06:39:09.383                1
0      9.24.255.255/32                       0x78f2fd344838 0x0    0    0
  2023/03/14 06:38:38.931                1
0      10.64.69.164/32                          0x78f2fd33fac8 0x0    0    0
  2023/03/14 06:39:09.383                1
0      10.77.128.69/32                          0x78f2fd3420a8 0x0    0    0
```

```

2023/03/14 06:39:09.383      1
0 240.0.0.0/4                0x78f2fd34f4d8 0x0      0      0
2023/03/14 06:38:18.686      1
0 10.106.26.249/32          0x78f2fd3399a8 0x0      0      0
2023/03/14 06:39:09.383      1
0 0.0.0.0/32                0x78f2fd34a768 0x0      0      0
2023/03/14 06:38:18.685      1
0 9.24.23.30/32            0x78f2fd1f2078 0x0      0      0
2023/03/14 06:38:38.930     24
0 9.24.0.0/16              0x78f2fd33af48 0x0      0      0
2023/03/14 06:38:38.930      1
0 0.0.0.0/8                0x78f2fd34fb48 0x0      0      0
2023/03/14 06:38:18.686      1

```

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 11: show platform software fed switch active ip route のフィールドの説明

フィールド	説明
vrf	VRF ID。
dest	宛先アドレス。
htm	IP ルートのハッシュテーブルマネージャオブジェクトポインタ。
SGT	セキュリティグループタグ。
DGID	接続先タグ ID。

show platform software fed switch active sgacl detail

ポリシー情報やカウント情報とともにグローバル適用ステータスを表示するには、特権EXECモードで **show platform software fed switch active sgacl detail** コマンドを使用します。

show platform software fed switch active sgacl detail

Syntax Description

sgacl SGACLハードウェア情報を表示します。

detail 詳細な SGACL 情報を表示します。

Command Modes

特権 EXEC (#)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.1

このコマンドが導入されました。

例

次に、**show platform software fed switch active sgacl detail** コマンドの出力例を示します。

```
Device# show platform software fed switch active sgacl detail
Global Enforcement: Off

*Refcnt: for the non-SGACL feature
===== DGID Table =====
SGT/Refcnt      DGT      DGID      test_cell monitor  permitted  denied
=====
*/3              2         1
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 12: show platform software fed switch active sgacl detail のフィールドの説明

フィールド	説明
SGT/Refcnt	セキュリティグループのタグ/強化。
DGT	接続先タグ。
DGID	接続先タグ ID。

show platform software fed switch active sgACL port

すべてのインターフェイスのレイヤ2インターフェイス設定項目およびステータスを表示するには、特権 EXEC モードで **show platform software fed switch active sgACL port** コマンドを使用します。

show platform software fed switch active sgACL port

Syntax Description	sgACL	セキュリティ グループ アクセス コントロール リスト (SGACL) のハードウェア情報を表示します。
	port	ポート構成を指定します。
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active sgACL port** コマンドの出力例を示します。

```
Device# show platform software fed switch active sgACL port
```

Port	Status	Port-SGT	Trust	Propagate	IngressCache	EgressCache
Gi3/0/1	Disabled	0	No	No	No	No
Gi3/0/2	Disabled	0	No	No	No	No
Gi3/0/3	Disabled	0	No	No	No	No
Gi3/0/4	Disabled	0	No	No	No	No
Gi3/0/5	Disabled	0	No	No	No	No
Gi3/0/6	Disabled	0	No	No	No	No
Gi3/0/7	Disabled	0	No	No	No	No
Gi3/0/8	Disabled	0	No	No	No	No
Gi3/0/9	Disabled	0	No	No	No	No
Gi3/0/10	Disabled	0	No	No	No	No
Gi3/0/11	Disabled	0	No	No	No	No
Gi3/0/12	Disabled	0	No	No	No	No
Gi3/0/13	Disabled	0	No	No	No	No
Gi3/0/14	Disabled	0	No	No	No	No
Gi3/0/15	Disabled	0	No	No	No	No
Gi3/0/16	Disabled	0	No	No	No	No
Gi3/0/17	Disabled	0	No	No	No	No
Gi3/0/18	Disabled	0	No	No	No	No
Gi3/0/19	Disabled	0	No	No	No	No
Gi3/0/20	Disabled	0	No	No	No	No
Gi3/0/21	Disabled	0	No	No	No	No
Gi3/0/22	Disabled	0	No	No	No	No
Gi3/0/23	Disabled	0	No	No	No	No
Gi3/0/24	Disabled	0	No	No	No	No
Gi3/0/25	Disabled	0	No	No	No	No
Gi3/0/26	Disabled	0	No	No	No	No
Gi3/0/27	Disabled	0	No	No	No	No
Gi3/0/28	Disabled	0	No	No	No	No
Gi3/0/29	Disabled	0	No	No	No	No
Gi3/0/30	Disabled	0	No	No	No	No

show platform software fed switch active sgACL port

Gi3/0/31	Disabled	0	No	No	No	No
Gi3/0/32	Disabled	0	No	No	No	No
Gi3/0/33	Disabled	0	No	No	No	No
Gi3/0/34	Disabled	0	No	No	No	No
Gi3/0/35	Disabled	0	No	No	No	No
Gi3/0/36	Disabled	0	No	No	No	No
Gi3/0/37	Disabled	0	No	No	No	No
Gi3/0/38	Disabled	0	No	No	No	No
Gi3/0/39	Disabled	0	No	No	No	No
Gi3/0/40	Disabled	0	No	No	No	No
Gi3/0/41	Disabled	0	No	No	No	No
Gi3/0/42	Disabled	0	No	No	No	No
Gi3/0/43	Disabled	0	No	No	No	No
Gi3/0/44	Disabled	0	No	No	No	No
Gi3/0/45	Disabled	0	No	No	No	No
Gi3/0/46	Disabled	0	No	No	No	No
Gi3/0/47	Disabled	0	No	No	No	No
Gi3/0/48	Disabled	0	No	No	No	No
Gi3/1/1	Disabled	0	No	No	No	No
Gi3/1/2	Disabled	0	No	No	No	No
Gi3/1/3	Disabled	0	No	No	No	No
Gi3/1/4	Disabled	0	No	No	No	No
Te3/1/1	Disabled	0	No	No	No	No
Te3/1/2	Disabled	0	No	No	No	No
Te3/1/3	Disabled	0	No	No	No	No
Te3/1/4	Disabled	0	No	No	No	No
Te3/1/5	Disabled	0	No	No	No	No
Te3/1/6	Disabled	0	No	No	No	No
Te3/1/7	Disabled	0	No	No	No	No
Te3/1/8	Disabled	0	No	No	No	No
Fo3/1/1	Disabled	0	No	No	No	No
Fo3/1/2	Disabled	0	No	No	No	No
Tw3/1/1	Disabled	0	No	No	No	No
Tw3/1/2	Disabled	0	No	No	No	No
Ap3/0/1	Disabled	0	No	No	No	No

出力フィールドの意味は自明です。

show platform software fed switch active sgacl vlan

VLANでのグローバル適用ステータスを表示するには、特権 EXEC モードで **show platform software fed switch active sgacl vlan** コマンドを使用します。

show platform software fed switch active sgacl vlan

Syntax Description

sgacl SGACLハードウェア情報を表示します。

vlan VLAN 設定を指定します。

Command Modes

特権 EXEC (#)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.1

このコマンドが導入されました。

例

次に、**show platform software fed switch active sgacl vlan** コマンドの出力例を示します。

```
Device# show platform software fed switch active sgacl vlan
```

```
Enforcement enabled:
```

```
vlan0  
vlan1  
vlan2  
vlan10  
vlan102  
vlan192  
vlan200
```

show platform software status control-processor brief

CPU とメモリに関する簡潔な情報を表示するには、特権 EXEC モードで **show platform software status control-processor brief** コマンドを使用します。

show platform software status control-processor brief

Syntax Description

status	システム ステータスを表示します。
control-processor	制御プロセッサのステータスを表示します。
brief	簡潔にステータスを表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software status control-processor brief** コマンドの出力例を示します。

```
Device# show platform software status control-processor brief
```

Load Average

```
Slot Status 1-Min 5-Min 15-Min
3-RP0 Healthy 0.03 0.07 0.04
```

Memory (kB)

```
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
3-RP0 Healthy 7745656 4178292 (54%) 3567364 (46%) 4755060 (61%)
```

CPU Utilization

```
Slot CPU User System Nice Idle IRQ SIRQ IOwait
3-RP0 0 0.50 0.40 0.00 99.10 0.00 0.00 0.00
      1 0.90 0.50 0.00 98.59 0.00 0.00 0.00
      2 0.40 0.40 0.00 99.20 0.00 0.00 0.00
      3 0.80 0.30 0.00 98.90 0.00 0.00 0.00
      4 0.60 0.30 0.00 99.09 0.00 0.00 0.00
      5 0.70 0.30 0.00 99.00 0.00 0.00 0.00
      6 1.20 0.30 0.00 98.50 0.00 0.00 0.00
      7 0.59 0.39 0.00 99.00 0.00 0.00 0.00
```

出力フィールドの意味は自明です。

show monitor capture <name> buffer

モニターキャプチャバッファまたはキャプチャポイントの内容を表示するには、特権 EXEC モードで **show monitor capture buffer name buffer** コマンドを使用します。

show monitor capture name buffer

Syntax Description	buffer	指定されたキャプチャバッファの内容を表示します。
	<i>name</i>	キャプチャバッファの名前を表します。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

次に、**show monitor capture name buffer** コマンドの出力例を示します。

```
Device# enable
Device# show monitor capture NewCapture buffer

Starting the packet display ..... Press Ctrl + Shift + 6 to exit

1 0.000000 10.4.1.117 -> 10.5.1.108 ICMP 124 Echo (ping) reply id=0x0008, seq=44279/63404,
   ttl=127
2 0.108862 10.4.1.113 -> 10.5.1.109 ICMP 124 Echo (ping) reply id=0x0008, seq=26717/23912,
   ttl=127
3 0.110106 10.4.1.119 -> 10.5.1.102 ICMP 124 Echo (ping) reply id=0x0008, seq=28341/46446,
   ttl=127
```

出力フィールドの意味は自明です。

timeout (CTS)

応答のタイムアウト（秒数）を設定するには、ポリシーサーバコンフィギュレーションモードで **timeout** コマンドを使用します。応答のタイムアウトをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*
no **timeout**

Syntax Description	<i>seconds</i>	秒単位のタイムアウト値です。 有効値は 1 ~ 60 です。
Command Default	デフォルトは 5 分です。	
Command Modes	ポリシーサーバ コンフィギュレーション (config-policy-server)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、ポリシーサーバのタイムアウトを変更する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# timeout 8
```

Related Commands	コマンド	説明
	cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。

tls server-trustpoint

Transport Layer Security (TLS) のトラストポイントを設定するには、ポリシーサーバコンフィギュレーションモードで **tls server-trustpoint** コマンドを使用します。TLS トラストポイントを削除するには、このコマンドの **no** 形式を使用します。

tls server-trustpoint *name*
no **tls server-trustpoint**

Syntax Description	<i>name</i>	トラストポイント名。
Command Default	TLS が設定されています。	
Command Modes	ポリシーサーバ コンフィギュレーション (config-policy-server)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines TLS は、Cisco Identity Services Engine (ISE) に接続するためにネットワークデバイスで使用されます。デバイスによる TLS 接続の確立には「Make or Break」のアプローチが使用され、デバイスと Cisco ISE の間に永続的な TLS 接続はありません。TLS 接続が確立された後、その接続を使用して、デバイスから特定の Uniform Resource Locator (URL) に複数の REST API コールを送信できます。すべての REST 要求が処理されると、サーバからの TCP-FIN メッセージによって接続が切断されます。新しい REST API コールを送信するには、サーバとの新しい接続を確立する必要があります。

無効なトラストポイントが設定されている場合、TLS ハンドシェイクは失敗し、サーバが停止中としてマークされます。

Examples

次に、TLS トラストポイントを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# tls server-trustpoint ise_trust
```

Related Commands	コマンド	説明
	cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバコンフィギュレーションモードを開始します。



PART III

インターフェイスおよびハードウェアコンポーネント

- [インターフェイスおよびハードウェア コマンド, on page 175](#)



インターフェイスおよびハードウェアコマンド

- [bluetooth pin, on page 178](#)
- [clear coap database, on page 179](#)
- [clear macro auto configuration, on page 180](#)
- [coap endpoint \(COAP プロキシ コンフィギュレーション\) , on page 181](#)
- [debug coap, on page 182](#)
- [device classifier, on page 183](#)
- [debug ilpower, on page 184](#)
- [debug interface, on page 185](#)
- [debug lldp packets, on page 187](#)
- [debug platform poe, on page 188](#)
- [debug platform software fed switch active punt packet-capture start, on page 189](#)
- [duplex, on page 191](#)
- [errdisable detect cause, on page 193](#)
- [errdisable recovery cause, on page 196](#)
- [errdisable recovery cause, on page 199](#)
- [interface, on page 202](#)
- [interface range, on page 205](#)
- [ip mtu, on page 207](#)
- [ipv6 mtu, on page 209](#)
- [list \(COAP プロキシ コンフィギュレーション\) , on page 211](#)
- [lldp \(インターフェイス コンフィギュレーション\) , on page 212](#)
- [logging event power-inline-status, on page 214](#)
- [macro, on page 215](#)
- [macro auto, on page 218](#)
- [macro auto apply \(Cisco IOS シェルのスクリプト機能\) , on page 221](#)
- [macro auto config \(Cisco IOS シェルのスクリプト機能\) , on page 223](#)
- [macro auto control, on page 224](#)
- [macro auto execute, on page 226](#)
- [macro auto global control, on page 233](#)
- [macro auto global processing, on page 235](#)

- macro auto mac-address-group, on page 236
- macro auto processing, on page 238
- macro auto sticky, on page 239
- macro auto trigger, on page 240
- macro description, on page 242
- macro global, on page 243
- macro global description, on page 246
- max-endpoints (COAP プロキシ コンフィギュレーション) , on page 247
- mdix auto, on page 248
- monitoring, on page 249
- network-policy, on page 251
- network-policy profile (グローバル コンフィギュレーション) , on page 252
- port-dtls (COAP プロキシ コンフィギュレーション) , on page 253
- port-unsecure (COAP プロキシ コンフィギュレーション) , on page 254
- power-priority , on page 255
- power inline, on page 257
- power inline police, on page 261
- power supply, on page 264
- power supply autoLC shutdown, on page 266
- resource directory (COAP プロキシ コンフィギュレーション) , on page 267
- security (COAP プロキシ コンフィギュレーション) , on page 268
- shell trigger, on page 269
- show beacon all, on page 271
- show coap dtls endpoints, on page 272
- show coap endpoints, on page 273
- show coap globals, on page 274
- show coap resources, on page 275
- show coap stats, on page 276
- show coap version, on page 277
- show device classifier attached, on page 278
- show device classifier clients, on page 280
- show device classifier profile type, on page 281
- show environment, on page 284
- show errdisable detect, on page 287
- show errdisable recovery, on page 289
- show ip interface, on page 290
- show interfaces, on page 296
- show interfaces counters, on page 303
- show interfaces switchport, on page 306
- show interfaces transceiver, on page 309
- show macro auto, on page 313
- show memory platform, on page 316
- show module, on page 319
- show network-policy profile, on page 320
- show parser macro, on page 321

- show platform hardware bluetooth, on page 324
- show platform hardware fed switch forward interface, on page 325
- show platform hardware fed switch fwd-asic counters tla, on page 328
- show platform hardware fed active fwd-asic resource team utilization, on page 332
- show platform resources, on page 334
- show platform software audit, on page 335
- show platform software fed switch punt cpuq rates, on page 339
- show platform software fed switch punt packet-capture display, on page 341
- show platform software fed switch punt rates interfaces, on page 343
- show platform software ilpower, on page 346
- show platform software memory, on page 348
- show platform software process list, on page 355
- show platform software process memory, on page 359
- show platform software process slot switch, on page 362
- show platform software status control-processor, on page 364
- show platform software thread list, on page 367
- show processes cpu platform, on page 369
- show processes cpu platform history, on page 372
- show processes cpu platform monitor, on page 375
- show processes memory, on page 377
- show processes memory platform, on page 381
- show processes platform, on page 385
- show shell, on page 388
- show system mtu, on page 391
- show tech-support , on page 392
- show tech-support bgp, on page 394
- show tech-support diagnostic, on page 398
- speed, on page 400
- start (COAP プロキシ コンフィギュレーション) , on page 402
- stop (COAP プロキシ コンフィギュレーション) , on page 403
- switchport block, on page 404
- system mtu, on page 406
- transport (COAP プロキシ コンフィギュレーション) , on page 407
- voice-signaling vlan (ネットワークポリシー コンフィギュレーション) , on page 408
- voice vlan (ネットワークポリシー コンフィギュレーション) , on page 410

bluetooth pin

新しい Bluetooth PIN を設定するには、モードまたはグローバル コンフィギュレーション モードで **bluetooth pin** コマンドを使用します。

bluetooth pin pin

Syntax Description	<i>pin</i>	Bluetooth インターフェイスのペアリング PIN。 PIN は 4 桁の番号です。
---------------------------	------------	--

Command Modes	グローバル コンフィギュレーション (config)
----------------------	----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

Usage Guidelines **bluetooth pin** コマンドは、モードまたはグローバルコンフィギュレーションモードで設定できます。シスコでは、Bluetooth PIN の設定にはグローバルコンフィギュレーションモードを使用することを推奨しています。

Examples 次に、**bluetooth pin** コマンドを使用して新しい Bluetooth PIN を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# bluetooth pin 1111
Device(config)#
```

Related Commands	コマンド	説明
	show platform hardware bluetooth	Bluetooth インターフェイスに関する情報を表示します。

clear coap database

CoAP データベースをクリアするには、ユーザ EXEC モードまたは特権 EXEC モードで **clear coap database** コマンドを使用します。

clear coap database

Command Default

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、CoAP データベースをクリアする例を示します。

```
Device(config)# clear coap database
```

clear macro auto configuration

マクロによって適用された設定をインターフェイスから削除するには、**clear macro auto configuration** コマンドを使用します。



Note **clear macro auto configuration** コマンドを実行する前に、スイッチで Auto SmartPort を無効にする必要があります。

clear macro auto configuration {all | interface [*interface-id*]}

Syntax Description	<i>all</i>	すべてのインターフェイスからマクロによって適用された設定を削除します。
	interface [<i>interface-id</i>]	インターフェイスからマクロによって適用された設定を削除します。

Command Default このコマンドにはデフォルト設定はありません。

Command Modes ユーザ EXEC (>)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、スイッチのすべてのインターフェイスまたは特定のインターフェイスからマクロによって適用された設定を削除するために使用します。

設定を確認するには、特権 EXEC モードで **show macro auto interface** コマンドを入力します。

例

次に、スイッチインターフェイスから設定を削除する例を示します。

```
Device(config)# clear macro auto configuration all
```

coap endpoint (COAP プロキシ コンフィギュレーション)

複数の IPv4/IPv6 スタティックエンドポイントをサポートするように COAP プロキシを設定するには、COAP プロキシ コンフィギュレーション モードで **coap endpoint** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
coap endpoint {ipv4 | ipv6}[ip-address]
no coap endpoint {ipv4 | ipv6}[ip-address]
```

Syntax Description	ipv4 <i>ip-address</i>	IPv4 スタティックエンドポイントを指定します。
	ipv6 <i>ip-address</i>	IPv6 スタティックエンドポイントを指定します。
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、IPv4 スタティックエンドポイントを設定する例を示します。

```
Device(config)# endpoint ipv4 192.168.255.1
Device(config-coap-proxy)# transport tcp
```

debug coap

COAP 設定のデバッグをイネーブルにするには、特権 EXEC モードで **debug coap** コマンドを使用します。

debug coap {all | database | errors | events | packet | trace | warnings}

Syntax Description		
all		すべての COAP デバッグメッセージを表示します。
database		COAP データベース デバッグ メッセージを表示します。
errors		COAP エラーデバッグメッセージを表示します。
events		COAP イベントデバッグメッセージを表示します。
packet		COAP パケットデバッグメッセージを表示します。
trace		COAP トレースデバッグメッセージを表示します。
warnings		COAP 警告デバッグメッセージを表示します。

Command Default このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、COAP データベースのデバッグをイネーブルにする例を示します。

```
Device# debug coap database
```

device classifier

デバイス分類子をイネーブルにするには、グローバル コンフィギュレーション モードで **device classifier** コマンドを使用します。デバイス分類子をディセーブルにするには、このコマンドの **no** 形式を使用します。

device classifier

no device classifier

Command Default

このコマンドは、デフォルトでは無効になっています。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デバイス分類子をディセーブルにするには、グローバル コンフィギュレーション モードで **no device classifier** コマンドを使用します。Auto SmartPort (ASP) などの機能が使用中のデバイス分類子はディセーブルにできません。

例

次に、スイッチの ASP デバイス分類子をイネーブルにする例を示します。

```
Device(config)# device classifier  
Device(config)# end
```

debug ilpower

電源コントローラおよびPower over Ethernet (PoE) システムのデバッグをイネーブルにするには、特権 EXEC モードで **debug ilpower** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug ilpower {cdp | event | ha | port | powerman | registries | scp | sense}
no debug ilpower {cdp | event | ha | port | powerman | registries | scp | sense}
```

Syntax Description

cdp	PoE Cisco Discovery Protocol (CDP) デバッグ メッセージを表示します。
event	PoE イベント デバッグ メッセージを表示します。
ha	PoE ハイ アベイラビリティ メッセージを表示します。
port	PoE ポート マネージャ デバッグ メッセージを表示します。
powerman	PoE 電力管理デバッグ メッセージを表示します。
registries	PoE レジストリ デバッグ メッセージを表示します。
scp	PoE SCP デバッグ メッセージを表示します。
sense	PoE sense デバッグ メッセージを表示します。

Command Default

デバッグはディセーブルです。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、PoE 対応スイッチだけでサポートされています。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタックメンバのデバッグを有効にする場合は、**session switch-number EXEC** コマンドを使用して、アクティブスイッチからのセッションを開始できます。次に、スタックメンバのコマンドラインプロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、アクティブスイッチ上で **remote command stack-member-number LINE EXEC** コマンドを使用します。

debug interface

インターフェイス関連アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug interface** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug interface {interface-id | counters {exceptions | protocol memory} | null interface-number |
port-channel port-channel-number | states | vlan vlan-id}
no debug interface {interface-id | counters {exceptions | protocol memory} | null interface-number |
port-channel port-channel-number | states | vlan vlan-id}
```

Syntax Description

<i>interface-id</i>	物理インターフェイスの ID です。タイプ スイッチ番号/モジュール番号/ポート（例：gigabitethernet 1/0/2）によって識別される指定された物理ポートのデバッグ メッセージを表示します。
null interface-number	スルインターフェイスのデバッグ メッセージを表示します。インターフェイス番号は常に 0 です。
port-channel <i>port-channel-number</i>	指定された EtherChannel ポートチャネルインターフェイスのデバッグ メッセージを表示します。 <i>port-channel-number</i> は 1 ～ 48 です。
vlan vlan-id	指定した VLAN のデバッグ メッセージを表示します。指定できる VLAN 範囲は 1 ～ 4094 です。
counters	カウンタ デバッグ情報を表示します。
exceptions	インターフェイスパケットおよびデータ レート統計情報の計算中に回復可能な例外条件が発生したときにデバッグ メッセージを表示します。
protocol memory	プロトコル カウンタのメモリ操作のデバッグ メッセージを表示します。
states	インターフェイスの状態が移行するときに中間のデバッグ メッセージを表示します。

Command Default

デバッグはディセーブルです。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

キーワードを指定しない場合は、すべてのデバッグ メッセージが表示されます。

undebg interface コマンドは **no debug interface** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタックメンバのデバッグを有効にする場合は、**session switch-number EXEC** コマンドを使用して、アクティブスイッチからのセッションを開始できます。次に、スタックメンバのコマンドラインプロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、アクティブスイッチ上で **remote command stack-member-number LINE EXEC** コマンドを使用します。

debug lldp packets

Link Layer Discovery Protocol (LLDP) パケットのデバッグをイネーブルにするには、特権 EXEC モードで **debug lldp packets** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug lldp packets
no debug lldp packets

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

デバッグはディセーブルです。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

undebug lldp packets コマンドは **no debug lldp packets** コマンドと同じです。

あるスイッチスタック上でデバッグをイネーブルにした場合は、アクティブスイッチでのみイネーブルになります。スタックメンバのデバッグを有効にする場合は、**session switch-number EXEC** コマンドを使用して、アクティブスイッチからのセッションを開始できます。

debug platform poe

Power over Ethernet (PoE) ポートのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform poe** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

```
debug platform poe [error | info] [switch switch-number]
no debug platform poe [error | info] [switch switch-number]
```

Syntax Description	error	(任意) PoE 関連エラーのデバッグ メッセージを表示します。
	info	(任意) PoE 関連情報のデバッグ メッセージを表示します。
	switch switch-number	(任意) スタック メンバを指定します。このキーワードは、スタック対応スイッチでのみサポートされています。
Command Default	デバッグはディセーブルです。	
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	undebg platform poe コマンドは no debug platform poe コマンドと同じです。	

debug platform software fed switch active punt packet-capture start

アクティブスイッチのCPU使用率が高いときのパケットのデバッグを有効にするには、特権 EXEC モードで **debug platform software fed switch active punt packet-capture start** コマンドを使用します。アクティブスイッチのCPU使用率が高いときのパケットのデバッグを無効にするには、特権 EXEC モードで **debug platform software fed switch active punt packet-capture stop** コマンドを使用します。

debug platform software fed switch active punt packet-capture start
debug platform software fed switch active punt packet-capture stop

Syntax Description

switch active	アクティブスイッチに関する情報を表示します。
punt	パント情報を指定します。
packet-capture	キャプチャされたパケットに関する情報を指定します。
start	アクティブスイッチのデバッグを有効にします。
stop	アクティブスイッチのデバッグを無効にします。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines

debug platform software fed switch active punt packet-capture start コマンドを設定すると、CPU 使用率が高いときにパケットのデバッグが開始されます。バッファサイズが 4K を超えるとパケットキャプチャが停止します。

Examples

次に、**debug platform software fed switch active punt packet-capture start** コマンドの出力例を示します。

```
Device# debug platform software fed switch active packet-capture start
Punt packet capturing started.
```

次に、**debug platform software fed switch active punt packet-capture stop** コマンドの出力例を示します。

```
debug platform software fed switch active punt packet-capture start
```

```
Device# debug platform software fed switch active packet-capture stop  
Punt packet capturing stopped. Captured 101 packet(s)
```

duplex

ポートのデュプレックスモードで動作するように指定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
duplex {auto | full | half}
no duplex {auto | full | half}
```

Syntax Description

auto 自動によるデュプレックス設定をイネーブルにします。接続されたデバイスモードにより、ポートが自動的に全二重モードか半二重モードで動作すべきかを判断します。

full 全二重モードをイネーブルにします。

half 半二重モードをイネーブルにします（10 または 100 Mb/s で動作するインターフェイスに限る）。1000 Mb/s、10,000 Mb/s、2.5Gb/s、5Gb/s で動作するインターフェイスに対しては半二重モードを設定できません。

Command Default

ギガビットイーサネット ポートのデフォルトは **auto** です。

二重オプションは、1000BASE-*x* または 10GBASE-*x*（-*x* は -BX、-CWDM、-LX、-SX、または -ZX） SFP モジュールではサポートされていません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ギガビットイーサネット ポートでは、接続装置がデュプレックスパラメータの自動ネゴシエーションを行わない場合にポートを **auto** に設定すると、**full** を指定するのと同じ効果があります。



Note デュプレックスモードが **auto** で接続されている装置が半二重で動作している場合、半二重モードはギガビットイーサネットインターフェイスでサポートされます。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

両方のラインの終端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にあるデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。



Caution インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

Examples

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Devic(config-if)# duplex full
```

errdisable detect cause

特定の原因またはすべての原因に対して errdisable 検出をイネーブルにするには、グローバルコンフィギュレーションモードで **errdisable detect cause** コマンドを使用します。errdisable 検出機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
errdisable detect cause {all|arp-inspection|bpduguard shutdown vlan|dhcp-rate-limit|dtp-flap|gbic-invalid|inline-power|link-flap|loopback|pagp-flap|pppoe-ia-rate-limit|psp shutdown vlan|security-violation shutdown vlan|sfp-config-mismatch}
no errdisable detect cause {all|arp-inspection|bpduguard shutdown vlan|dhcp-rate-limit|dtp-flap|gbic-invalid|inline-power|link-flap|loopback|pagp-flap|pppoe-ia-rate-limit|psp shutdown vlan|security-violation shutdown vlan|sfp-config-mismatch}
```

Syntax Description

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミックアドレス解決プロトコル (ARP) インспекションのエラー検出をイネーブルにします。
bpduguard shutdown vlan	BPDU ガードで VLAN ごとに errdisable をイネーブルにします。
dhcp-rate-limit	Dynamic Host Configuration Protocol (DHCP) スヌーピング用のエラー検出をイネーブルにします。
dtp-flap	ダイナミック トランッキング プロトコル (DTP) フラップのエラー検出をイネーブルにします。
gbic-invalid	無効なギガビットインターフェイス コンバータ (GBIC) モジュール用のエラー検出をイネーブルにします。 Note このエラーは、無効な Small Form-Factor Pluggable (SFP) モジュールを意味します。
inline-power	Power over Ethernet (PoE) の errdisable 原因に対して、エラー検出をイネーブルにします。 Note このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。
link-flap	リンクステートのフラップに対して、エラー検出をイネーブルにします。
loopback	検出されたループバックに対して、エラー検出をイネーブルにします。
pagp-flap	ポート集約プロトコル (PAgP) フラップの errdisable 原因のエラー検出をイネーブルにします。

pppoe-ia-rate-limit	PPPoE 中継エージェントのレート制限 errdisable 原因に対して、エラー検出をイネーブルにします。
psp shutdown vlan	プロトコル ストーム プロテクション (PSP) のエラー検出をイネーブルにします。
security-violation shutdown vlan	音声認識 IEEE 802.1X セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。

Command Default

検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

原因 (link-flap、dhcp-rate-limit など) は、errdisable ステートが発生した理由です。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステートとなり、リンクダウンステートに類似した動作ステートとなります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。ブリッジプロトコル データ ユニット (BPDU) ガード、音声認識 802.1X セキュリティ、およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN のみをシャットダウンするようにスイッチを設定できます。

errdisable recovery グローバル コンフィギュレーション コマンドを入力して、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、インターフェイスは errdisable ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、インターフェイスを手動で errdisable ステートから回復させる必要があります。

プロトコル ストーム プロテクションでは、最大 2 個の仮想ポートについて過剰なパケットがドロップされます。**psp** キーワードを使用した仮想ポートの errdisable は、EtherChannel および Flexlink インターフェイスではサポートされません。

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

次の例では、リンクフラップ errdisable 原因に対して errdisable 検出をイネーブルにする方法を示します。

```
Device (config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの errdisable ステートで BPDU ガードをグローバルに設定する方法を示します。

```
Device(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドでは、VLAN ごとの errdisable ステートで音声認識 802.1X セキュリティをグローバルに設定する方法を示します。

```
Device(config)# errdisable detect cause security-violation shutdown vlan
```

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

errdisable recovery cause

特定の原因から回復するように errdisable メカニズムをイネーブルにするには、グローバル コンフィギュレーションモードで **errdisable recovery cause** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure |
pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control |
udld}
no errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure |
pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control |
udld}
```

Syntax Description	all	すべての errdisable の原因から回復するタイマーをイネーブルにします。
	arp-inspection	アドレス解決プロトコル (ARP) 検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
	bpduguard	ブリッジプロトコルデータユニット (BPDU) ガード errdisable ステートから回復するタイマーをイネーブルにします。
	channel-misconfig	EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
	dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。
	dtp-flap	ダイナミック トランッキングプロトコル (DTP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。
	gbic-invalid	ギガビット インターフェイス コンバータ (GBIC) モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 Note このエラーは無効な Small Form-Factor Pluggable (SFP) の errdisable ステートを意味します。
	inline-power	Power over Ethernet (PoE) の errdisable ステートから回復するタイマーをイネーブルにします。 このキーワードは、PoEポートを備えたスイッチでのみサポートされています。

link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
mac-limit	MAC 制限 errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	ポート集約プロトコル (PAgP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。
port-mode-failure	ポートモードの変更失敗の errdisable ステートから回復するタイマーをイネーブルにします。
pppoe-ia-rate-limit	PPPoE IA レート制限 errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポートセキュリティ違反ディセーブルステートから回復するタイマーをイネーブルにします。
psp	プロトコル ストーム プロテクション (PSP) の errdisable ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1X 違反ディセーブルステートから回復するタイマーをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。
storm-control	ストーム制御エラーから回復するタイマーをイネーブルにします。
udld	単方向リンク検出 (UDLD) errdisable ステートから回復するタイマーをイネーブルにします。

Command Default すべての原因に対して回復はディセーブルです。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 原因 (all、BDPU ガードなど) は、errdisable ステートが発生した理由として定義されます。原因がインターフェイスで検出された場合、インターフェイスはerrdisableステート (リンクダウンスステートに類似した動作ステート) となります。

ポートが **errdisable** になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

原因の回復をイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで **errdisable** ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは **errdisable** ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でインターフェイスを **errdisable** ステートから回復させる必要があります。

設定を確認するには、**show errdisable recovery** 特権 EXEC コマンドを入力します。

Examples

次の例では、BPDU ガード **errdisable** 原因に対して回復タイマーをイネーブルにする方法を示します。

```
Device# Device#configure terminal
Device(config)# errdisable recovery cause bpduguard
```

errdisable recovery cause

特定の原因から回復するように errdisable メカニズムをイネーブルにするには、グローバル コンフィギュレーションモードで **errdisable recovery cause** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure |
pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control |
udld}
```

```
no errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure |
pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control |
udld}
```

Syntax Description

all	すべての errdisable の原因から回復するタイマーをイネーブルにします。
arp-inspection	アドレス解決プロトコル (ARP) 検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
bpduguard	ブリッジプロトコルデータユニット (BPDU) ガード errdisable ステートから回復するタイマーをイネーブルにします。
channel-misconfig	EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。
dtp-flap	ダイナミック トランキンング プロトコル (DTP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。
gbic-invalid	ギガビット インターフェイス コンバータ (GBIC) モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 Note このエラーは無効な Small Form-Factor Pluggable (SFP) の errdisable ステートを意味します。
inline-power	Power over Ethernet (PoE) の errdisable ステートから回復するタイマーをイネーブルにします。 このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。

link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
mac-limit	MAC 制限 errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	ポート集約プロトコル (PAgP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。
port-mode-failure	ポートモードの変更失敗の errdisable ステートから回復するタイマーをイネーブルにします。
pppoe-ia-rate-limit	PPPoE IA レート制限 errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポートセキュリティ違反ディセーブルステートから回復するタイマーをイネーブルにします。
psp	プロトコル ストーム プロテクション (PSP) の errdisable ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1X 違反ディセーブルステートから回復するタイマーをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。
storm-control	ストーム制御エラーから回復するタイマーをイネーブルにします。
udld	単方向リンク検出 (UDLD) errdisable ステートから回復するタイマーをイネーブルにします。

Command Default すべての原因に対して回復はディセーブルです。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 原因 (all、BDPU ガードなど) は、errdisable ステートが発生した理由として定義されます。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステート (リンクダウンステートに類似した動作ステート) となります。

ポートが **errdisable** になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

原因の回復をイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで **errdisable** ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは **errdisable** ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でインターフェイスを **errdisable** ステートから回復させる必要があります。

設定を確認するには、**show errdisable recovery** 特権 EXEC コマンドを入力します。

Examples

次の例では、BPDU ガード **errdisable** 原因に対して回復タイマーをイネーブルにする方法を示します。

```
Device# Device#configure terminal
Device(config)# errdisable recovery cause bpduguard
```

interface

インターフェイスを設定するには、**interface** コマンドを使用します。

interface { **AccessTunnel** *interface-number* | **Auto-Template** *interface-number* | **GigabitEthernet** *switch-number/slot-number/port-number* | **Internal Interface** *Internal Interface number* | **LISP** *interface-number* | **Loopback** *interface-number* | **Null** *interface-number* | **Port-channel** *interface-number* | **TenGigabitEthernet** *switch-number/slot-number/port-number* | **TwentyFiveGigE** *switch-number/slot-number/port-number* | **Tunnel** *interface-number* | **Vlan** *interface-number* }

Syntax Description

AccessTunnel <i>interface-number</i>	アクセス トンネル インターフェイスを設定できます。
Auto-Template <i>interface-number</i>	自動テンプレート インターフェイスを設定できます。範囲は 1 ~ 999 です。
GigabitEthernet <i>switch-number/slot-number/port-number</i>	ギガビットイーサネット IEEE 802.3z インターフェイスを設定できます。 <ul style="list-style-type: none"> • switch-number: スイッチ ID。有効な範囲は 1 ~ 8 です。 • slot-number: スロット番号。値の範囲は 0 ~ 1 です。 • port-number: ポート番号。有効な範囲は 1 ~ 48 です。
LISP <i>interface-number</i>	LISP インターフェイスを設定できます。
Loopback <i>interface-number</i>	ループバック インターフェイスを設定できます。指定できる範囲は 0 ~ 2147483647 です。
Null <i>interface-number</i>	ヌルインターフェイスを設定できます。デフォルト値は 0 です。
Port-channel <i>interface-number</i>	ポートチャネルインターフェイスを設定できます。有効な範囲は 1 ~ 128 です。

<p>TenGigabitEthernet <i>switch-number/slot-number/port-number</i></p>	<p>10 ギガビット イーサネット インターフェイスを設定できます。</p> <ul style="list-style-type: none"> • <i>switch-number</i>: スイッチ ID。有効な範囲は 1 ~ 8 です。 • <i>slot-number</i> : スロット番号。値の範囲は 0 ~ 1 です。 • <i>port-number</i>: ポート番号。範囲は 1 ~ 4、17 ~ 24、および 37 ~ 48 です。
<p>TwentyFiveGigE <i>switch-number/slot-number/port-number</i></p>	<p>25 ギガビット イーサネット インターフェイスを設定できます。</p> <ul style="list-style-type: none"> • <i>switch-number</i>: スイッチ ID。有効な範囲は 1 ~ 8 です。 • <i>slot-number</i>: スロット番号。値は 1 です。 • <i>port-number</i>: ポート番号。有効な範囲は 1 ~ 2 です。
<p>Tunnel <i>interface-number</i></p>	<p>トンネルインターフェイスを設定できます。指定できる範囲は 0 ~ 2147483647 です。</p>
<p>Vlan <i>interface-number</i></p>	<p>スイッチ VLAN を設定できます。指定できる範囲は 1 ~ 4094 です。</p>

Command Default

なし

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	TwentyFiveGigE キーワードがこのコマンドに追加されました。

Usage Guidelines

このコマンドは「no」形式を使用できません。
 アップリンクポートの範囲は 0 ~ 4 です。
 24 ポートスイッチのマルチギガビット イーサネット ポートの範囲は 17 ~ 24 です。
 48 ポートスイッチのマルチギガビット イーサネット ポートの範囲は 41 ~ 48 です。

Examples

次に、トンネルインターフェイスを設定する例を示します。

```
Device(config)# interface Tunnel 15  
Device(config-if)#
```

次に、25 ギガビット イーサネット インターフェイスを設定する例を示します。

```
Device(config)# interface TwentyFiveGigE 1/1/1  
Device(config-if)#
```

次に、40 ギガビット イーサネット インターフェイスを設定する例を示します。

interface range

インターフェイス範囲を設定するには、**interface range** コマンドを使用します。

interface range { **GigabitEthernet** *switch-number/slot-number/port-number* | **Loopback** *interface-number* **Null** *interface-number* **Port-channel** *interface-number* **TenGigabitEthernet** *switch-number/slot-number/port-number* **TwentyFiveGigE** *switch-number/slot-number/port-number* **Tunnel** *interface-number* **Vlan** *interface-number* }

Syntax Description

GigabitEthernet

switch-number/slot-number/port-number

ギガビットイーサネット IEEE 802.3z インターフェイスを設定できます。

- **switch-number:** スイッチ ID。有効な範囲は 1 ~ 8 です。
- **slot-number:** スロット番号。値の範囲は 0 ~ 1 です。
- **port-number:** ポート番号。指定できる範囲は 0 ~ 48 です。

Loopback *interface-number*

ループバック インターフェイスを設定できます。指定できる範囲は 0 ~ 2147483647 です。

Port-channel *interface-number*

ポートチャネルインターフェイスを設定できます。有効な範囲は 1 ~ 48 です。

TenGigabitEthernet

switch-number/slot-number/port-number

10 ギガビットイーサネット インターフェイスを設定できます。

- **switch-number:** スイッチ ID。有効な範囲は 1 ~ 8 です。
- **slot-number**
: スロット番号。値の範囲は 0 ~ 1 です。
- **port-number:** ポート番号。範囲は 1 ~ 4、17 ~ 24、および 37 ~ 48 です。

TwentyFiveGigE

switch-number/slot-number/port-number

25 ギガビットイーサネット インターフェイスを設定できます。

- **switch-number:** スイッチ ID。有効な範囲は 1 ~ 8 です。
- **slot-number:** スロット番号。値は 1 です。
- **port-number:** ポート番号。有効な範囲は 1 ~ 2 です。

interface range

Tunnel *interface-number* トンネルインターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。

Vlan *interface-number* スイッチ VLAN を設定できます。指定できる範囲は 1 ～ 4094 です。

Command Default なし

Command Modes グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	TwentyFiveGigE キーワードがこのコマンドに追加されました。

Usage Guidelines アップリンクポートの範囲は 0 ～ 4 です。
 24 ポートスイッチのマルチギガビットイーサネットポートの範囲は 17 ～ 24 です。
 48 ポートスイッチのマルチギガビットイーサネットポートの範囲は 41 ～ 48 です。

Examples 次に、インターフェイス範囲を設定する例を示します。
 Device(config)# **interface range vlan 1-100**

ip mtu

スイッチまたはスイッチスタックのすべてのルーテッドポートのルーテッドパケットの IP 最大伝送ユニット (MTU) サイズを設定するには、インターフェイス コンフィギュレーション モードで **ip mtu** コマンドを使用します。デフォルトの IP MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ip mtu bytes
no ip mtu bytes

Syntax Description

bytes MTU サイズ (バイト単位)。指定できる範囲は 68 からシステム MTU 値 (バイト単位) までです。

Command Default

すべてのスイッチインターフェイスで送受信されるフレームのデフォルト IP MTU サイズは、1500 バイトです。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IP 値の上限は、スイッチまたはスイッチスタックの設定に基づき、現在適用されているシステム MTU 値を参照します。MTU サイズの設定に関する詳細については、**system mtu** グローバル コンフィギュレーション コマンドを参照してください。

デフォルトの IP MTU 設定に戻すには、インターフェイスで **default ip mtu** コマンドまたは **no ip mtu** コマンドを適用します。

設定を確認するには、**show ip interface interface-id** または **show interfaces interface-id** 特権 EXEC コマンドを入力します。

次に、VLAN 200 の最大 IP パケットサイズを 1000 バイト に設定する例を示します。

```
Device(config)# interface vlan 200
Device(config-if)# ip mtu 1000
```

次に、VLAN 200 の最大 IP パケットサイズをデフォルト設定の 1500 バイト に設定する例を示します。

```
Device(config)# interface vlan 200
Device(config-if)# default ip mtu
```

次に、**show ip interface interface-id** コマンドの出力の一部を示します。インターフェイスの現在の IP MTU 設定が表示されます。

```
Device# show ip interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
```

<output truncated>

ipv6 mtu

スイッチまたはスイッチスタックのすべてのルーテッドポートのルーテッドパケットのIPv6最大伝送ユニット (MTU) サイズを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mtu** コマンドを使用します。デフォルトの IPv6 MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ipv6 mtu bytes
no ipv6 mtu bytes

Syntax Description

bytes MTU サイズ (バイト単位)。指定できる範囲は1280からシステムMTU値 (バイト単位) までです。

Command Default

すべてのスイッチ インターフェイスで送受信されるフレームのデフォルト IPv6 MTU サイズは、1500 バイトです。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IPv6 MTU 値の上限は、スイッチまたはスイッチ スタックの設定に基づき、現在適用されているシステム MTU 値を参照します。MTU サイズの設定に関する詳細については、**system mtu** グローバル コンフィギュレーション コマンドを参照してください。

デフォルトの IPv6 MTU 設定に戻すには、インターフェイスで **default ipv6 mtu** コマンドまたは **no ipv6 mtu** コマンドを適用します。

設定を確認するには、**show ipv6 interface interface-id** または **show interface interface-id** 特権 EXEC コマンドを入力します。

次に、インターフェイスの最大 IPv6 パケット サイズを 2000 バイトに設定する例を示します。

```
Device(config)# interface gigabitethernet4/0/1
Device(config-if)# ipv6 mtu 2000
```

次に、インターフェイスの最大 IPv6 パケット サイズをデフォルト設定の 1500 バイトに設定する例を示します。

```
Device(config)# interface gigabitethernet4/0/1
Device(config-if)# default ipv6 mtu
```

次に、**show ipv6 interface interface-id** コマンドの出力の一部を示します。インターフェイスの現在の IPv6 MTU 設定が表示されます。

```
Device# show ipv6 interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
```

```
<output truncated>
```

list (COAP プロキシ コンフィギュレーション)

ライトとリソースを学習できる IP アドレス範囲を制限するには、COAP プロキシ コンフィギュレーションモードで **list** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

list コマンドを使用して、ipv4 または ipv6 に関係なく、最大 5 つの IP リストを設定できます。

```
list {ipv4 | ipv6}[list-name]
no list {ipv4 | ipv6}[list-name]
```

Syntax Description	ipv4 <i>list-name</i>	IPv4 リスト名を指定します。
	ipv6 <i>list-name</i>	IPv6 リスト名を指定します。
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	COAP プロキシ コンフィギュレーションモードにアクセスするには、グローバル コンフィギュレーションモードで coap proxy コマンドを入力します。	

例

次に、リスト名を使用して IPv4 アドレス範囲を制限する例を示します。

```
Device(config)# coap proxy
Device config-coap-proxy)# list ipv4 trial_list
```

lldp (インターフェイス コンフィギュレーション)

インターフェイスの Link Layer Discovery Protocol (LLDP) をイネーブルにするには、インターフェイス コンフィギュレーションモードで **lldp** コマンドを使用します。インターフェイスで LLDP をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
lldp {med-tlv-select tlv | receive | tlv-select power-management | transmit}
no lldp {med-tlv-select tlv | receive | tlv-select power-management | transmit}
```

Syntax Description

med-tlv-select	LLDP Media Endpoint Discovery (LLDP-MED) の Time Length Value (TLV) 要素を送信するように選択します。
<i>tlv</i>	TLV 要素を特定するストリング。有効な値は次のとおりです。 <ul style="list-style-type: none"> • inventory-management: LLDP MED インベントリ管理 TLV。 • location: LLDP MED ロケーション TLV。 • network-policy: LLDP MED ネットワーク ポリシー TLV。 • power-management: LLDP MED 電源管理 TLV。
receive	LLDP 伝送を受信するようにインターフェイスをイネーブルにします。
tlv-select	送信する LLDP TLV を選択します。
power-management	LLDP 電源管理 TLV を送信します。
transmit	インターフェイスで LLDP 伝送をイネーブルにします。

Command Default

LLDP はディセーブルです。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、802.1 メディア タイプでサポートされています。

インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。

インターフェイスの LLDP 伝送をディセーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no lldp transmit
```

インターフェイスの LLDP 伝送をイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# lldp transmit
```

logging event power-inline-status

Power over Ethernet (PoE) イベントのロギングをイネーブルにするには、インターフェイス コンフィギュレーションモードで **logging event power-inline-status** コマンドを使用します。PoE ステータス イベントのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging event power-inline-status
no logging event power-inline-status

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default PoE イベントのロギングはイネーブルです。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドの **no** 形式を使用しても、PoE エラーイベントはディセーブルになりません。

Examples

次の例では、ポート上で PoE イベントのロギングをイネーブルにする方法を示します。

```
Device(config-if)# interface gigabitethernet1/0/1
Device(config-if)# logging event power-inline-status
Device(config-if)#
```

macro

インターフェイスにマクロを適用するか、またはインターフェイス上のマクロを適用してデバッグするには、インターフェイス コンフィギュレーションモードで **macro** コマンドを使用します。

macro {**apply** | **trace**}*macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

Syntax Description		
apply		インターフェイスにマクロを適用します。
trace		インターフェイスにマクロを適用し、それをデバッグします。
<i>macro-name</i>		マクロ名を指定します。
parameter <i>value</i>		<p>(任意) インターフェイスに固有の一意のパラメータ値を指定します。最高3つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。</p> <p>キーワードで一致が見られると、すべて対応する値に置き換えられます。</p>

Command Default このコマンドにはデフォルト設定はありません。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **macro apply** *macro-name* コマンドを使用して、インターフェイス上で実行されているマクロを適用および表示できます。

macro trace *macro-name* コマンドを使用して、マクロを適用し、そのマクロをデバッグして構文エラーまたは設定エラーを判別できます。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをインターフェイスに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter value** キーワードを使用して、そのインターフェイスに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro apply macro-name ?** コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

スイッチソフトウェアには、シスコの SmartPort のマクロがデフォルトで組み込まれています。これらのマクロやコマンドは、ユーザ EXEC モードで **show parser macro** コマンドを使用して表示できます。

インターフェイスにシスコ デフォルト Smartport マクロを適用する場合は、次の注意事項に従ってください。

- スイッチ上のすべてのマクロを表示するには、ユーザ EXEC モードで **show parser macro** コマンドを使用します。特定のマクロの内容を表示するには、ユーザ EXEC モードで **show parser macro macro-name** コマンドを使用します。
- \$ で始まるキーワードには、一意のパラメータ値が必要です。**parameter value** キーワードを使用して、必要な値をシスコデフォルトマクロに追加します。

シスコデフォルトマクロは \$ という文字を使用しているため、必須キーワードを識別できます。\$ という文字を使用して、マクロを作成するときにキーワードを定義できます。

マクロをインターフェイスに適用する場合、マクロ名が自動的にインターフェイスに追加されません。ユーザ EXEC モードで **show running-config interface interface-id** コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

インターフェイスの範囲に適用されたマクロは、単一インターフェイスに適用されたマクロと同じ動作をします。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。1つのインターフェイスでマクロ コマンドの実行に失敗しても、マクロは残りのインターフェイス上に適用されます。

インターフェイス コンフィギュレーション モードで **default interface interface-id** コマンドを入力すれば、インターフェイスで適用されたマクロの設定を削除できます。

例

インターフェイス コンフィギュレーション モードで **macro name** コマンドを使用した後、インターフェイスに適用できます。次の例では、**duplex** という名前のユーザ作成マクロをインターフェイスに適用する方法を示します。

```
Device(config-if)# macro apply duplex
```

マクロをデバッグするには、インターフェイス コンフィギュレーション モードで **macro trace** コマンドを使用して、マクロがインターフェイスに適用されたときのマクロの構文または設定エラーを判別できます。

```
Device(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

次の例では、シスコデフォルト `cisco-desktop` マクロを表示する方法、およびインターフェイス上でマクロを適用し、アクセス VLAN ID を 25 に設定する方法を示します。

```
Device# show parser macro cisco-desktop
-----
Macro name : cisco-desktop
Macro type : default
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1
# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
-----
Device#
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet1/0/4
Device(config-if)# macro apply cisco-desktop $AVID 25
```

macro auto

CLI を使用してグローバルマクロを設定および適用するには、特権 EXEC モードで **macro auto** コマンドを使用します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

macro auto {**apply** | **config**} *macro-name*

Syntax Description		
apply		マクロを適用します。
config		マクロのパラメータを入力します。
<i>macro-name</i>		マクロ名を指定します。

Command Default スイッチにはマクロは適用されません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines スイッチからマクロを削除するには、マクロコマンドの **no** 形式を入力します。

macro auto config macro-name コマンドを入力すると、すべてのマクロパラメータの値を入力するよう要求されます。

macro-name を入力するときは文字列を正確に使用します。エントリは大文字と小文字が区別されます。

ユーザ定義の値は、**show macro auto** または **show running-config** コマンドの出力でのみ表示されます。

例

次に、グローバルマクロを表示する例を示します。

```
Device# macro auto apply ?
CISCO_SWITCH_AAA_ACCOUNTING          Configure aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION      Configure aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION       Configure aaa authorization parameters
CISCO_SWITCH_AUTO_IP_CONFIG          Configure the ip parameters
CISCO_SWITCH_AUTO_PCI_CONFIG         Configure PCI compliant parameters
CISCO_SWITCH_DOMAIN_NAME_CONFIG      Configure domain name
CISCO_SWITCH_ETHERCHANNEL_CONFIG     Configure the etherchannel parameters
CISCO_SWITCH_HOSTNAME_CONFIG         Configure hostname
CISCO_SWITCH_HTTP_SERVER_CONFIG      Configure http server
CISCO_SWITCH_LOGGING_SERVER_CONFIG   Configure logging server
```

```

CISCO_SWITCH_MGMT_VLAN_CONFIG      Configure management vlan parameters
CISCO_SWITCH_NAME_SERVER_CONFIG    Configure name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG      Configure NTP server
CISCO_SWITCH_RADIUS_SERVER_CONFIG   Configure radius server
CISCO_SWITCH_SETUP_SNMP_TRAPS       Configure SNMP trap parameters
CISCO_SWITCH_SETUP_USR_CONFIG       Configure the user parameters
CISCO_SWITCH_SNMP_SOURCE_CONFIG      Configure snmp source interface
CISCO_SWITCH_TACACS_SERVER_CONFIG    Configure tacacs server
CISCO_SWITCH_USER_PASS_CONFIG        Configure username and password

Device# macro auto config ?
CISCO_SWITCH_AAA_ACCOUNTING          Configure aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION      Configure aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION       Configure aaa authorization parameters
CISCO_SWITCH_AUTO_IP_CONFIG          Configure the ip parameters
CISCO_SWITCH_AUTO_PCI_CONFIG         Configure PCI compliant parameters
CISCO_SWITCH_DOMAIN_NAME_CONFIG      Configure domain name
CISCO_SWITCH_ETHERCHANNEL_CONFIG     Configure the etherchannel parameters
CISCO_SWITCH_HOSTNAME_CONFIG         Configure hostname
CISCO_SWITCH_HTTP_SERVER_CONFIG       Configure http server
CISCO_SWITCH_LOGGING_SERVER_CONFIG    Configure logging server
CISCO_SWITCH_MGMT_VLAN_CONFIG        Configure management vlan parameters
CISCO_SWITCH_NAME_SERVER_CONFIG      Configure name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG        Configure NTP server
CISCO_SWITCH_RADIUS_SERVER_CONFIG     Configure radius server
CISCO_SWITCH_SETUP_SNMP_TRAPS        Configure SNMP trap parameters
CISCO_SWITCH_SETUP_USR_CONFIG         Configure the user parameters
CISCO_SWITCH_SNMP_SOURCE_CONFIG       Configure snmp source interface
CISCO_SWITCH_TACACS_SERVER_CONFIG     Configure tacacs server
CISCO_SWITCH_USER_PASS_CONFIG         Configure username and password

```

次に、特定のマクロのパラメータを表示する例を示します。

```

Device# macro auto config CISCO_SWITCH_AUTO_IP_CONFIG ?
CISCO_SWITCH_DOMAIN_NAME_CONFIG      domain name parameters
CISCO_SWITCH_LOGGING_SERVER_CONFIG    logging host parameters
CISCO_SWITCH_NAME_SERVER_CONFIG       name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG        ntp server parameters
LINE                                  Provide parameters of form [Parameters
name=value]

<cr>

```

```

Device# macro auto config CISCO_SWITCH_AUTO_PCI_CONFIG ?
CISCO_SWITCH_AAA_ACCOUNTING          aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION      aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION       aaa authorization parameters
CISCO_SWITCH_HTTP_SERVER_CONFIG       http server parameters
CISCO_SWITCH_RADIUS_SERVER_CONFIG     radius server parameters
CISCO_SWITCH_TACACS_SERVER_CONFIG     tacacs server parameters
LINE                                  Provide parameters of form [Parameters
name=value]

<cr>

```

```

Device# macro auto config CISCO_SWITCH_SETUP_SNMP_TRAPS ?
CISCO_SWITCH_SNMP_SOURCE_CONFIG       snmp source parameters
LINE                                  Provide parameters of form [Parameters
name=value]

<cr>

```

```

Device# macro auto config CISCO_SWITCH_SETUP_USR_CONFIG ?CISCO_AUTO_TIMEZONE_CONFIG timezone
parameters
CISCO_SWITCH_HOSTNAME_CONFIG          hostname parameter

```

```

LINE                               Provide parameters of form [Parameters
                                   name=value]
<cr>

```

次に、マクロパラメータを設定し、CLIを使用してマクロを適用する例を示します。

```

Device# macro auto config CISCO_SWITCH_ETHERCHANNEL_CONFIG
Enter the port channel id[1-48] for 3K & 2350, [1-6] for 2K: 2
Enter the port channel type, Layer:[2-3(L3 not supported on 2K)]: 2
Enter etherchannel mode for the interface[auto/desirable/on/active/passive]: active
Enter the channel protocol[lacp/none]: lacp
Enter the number of interfaces to join the etherchannel[8-PAGE/MODE:ON,16-LACP]: 7
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/1
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/2
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/3
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/4
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/5
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/6
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/7
Do you want to apply the parameters? [yes/no]: yes
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Device# macro auto apply CISCO_SWITCH_ETHERCHANNEL_CONFIG
Enter configuration commands, one per line. End with CNTL/Z.
Device#

```

macro auto apply (Cisco IOS シェルのスクリプト機能)

Cisco IOS シェルのスクリプト機能を使用してグローバルマクロを設定および適用するには、特権 EXEC モードで **macro auto apply** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

macro auto apply *macro-name*

Syntax Description	apply	マクロを適用します。
	<i>macro-name</i>	マクロ名を指定します。
Command Default	スイッチにはマクロは適用されません。	
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スイッチからマクロを削除するには、マクロコマンドの **no** 形式を入力します。

macro-name を入力するときは文字列を正確に使用します。エントリは大文字と小文字が区別されます。

ユーザ定義の値は、**show macro auto** または **show running-config** コマンドの出力でのみ表示されます。

Cisco IOS シェルのスクリプト機能を使用してパラメータを設定することもできます。例については、「Configuring Auto Smartports and Static Smartports Macros」の章の「Configuring and Applying Global Macros」セクションを参照してください。

例

次に、グローバルマクロを表示する例を示します。

```
Device# macro auto apply ?
CISCO_SWITCH_AAA_ACCOUNTING      Configure aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION  Configure aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION   Configure aaa authorization parameters
CISCO_SWITCH_AUTO_IP_CONFIG      Configure the ip parameters
CISCO_SWITCH_AUTO_PCI_CONFIG     Configure PCI compliant parameters
CISCO_SWITCH_DOMAIN_NAME_CONFIG  Configure domain name
CISCO_SWITCH_ETHERCHANNEL_CONFIG Configure the etherchannel parameters
CISCO_SWITCH_HOSTNAME_CONFIG     Configure hostname
```

CISCO_SWITCH_HTTP_SERVER_CONFIG	Configure http server
CISCO_SWITCH_LOGGING_SERVER_CONFIG	Configure logging server
CISCO_SWITCH_MGMT_VLAN_CONFIG	Configure management vlan parameters
CISCO_SWITCH_NAME_SERVER_CONFIG	Configure name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG	Configure NTP server
CISCO_SWITCH_RADIUS_SERVER_CONFIG	Configure radius server
CISCO_SWITCH_SETUP_SNMP_TRAPS	Configure SNMP trap parameters
CISCO_SWITCH_SETUP_USR_CONFIG	Configure the user parameters
CISCO_SWITCH_SNMP_SOURCE_CONFIG	Configure snmp source interface
CISCO_SWITCH_TACACS_SERVER_CONFIG	Configure tacacs server
CISCO_SWITCH_USER_PASS_CONFIG	Configure username and password

macro auto config (Cisco IOS シェルのスクリプト機能)

グローバルマクロを設定および適用するには、特権 EXEC モードで **macro auto config** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

macro auto config *macro-name* [*parameter=value* [*parameter=value*]...]

Syntax Description	config	マクロのパラメータを入力します。
	<i>macro-name</i>	マクロ名を指定します。
	<i>parameter=value</i> [<i>parameter=value</i>] ...	parameter=value: グローバルマクロのパラメータ値の値を置き換えます。それぞれの名前と値のペアをスペースで区切る形式で新しい値を入力します (例: <name1>=<value1> [<name2>=<value2>...])。

Command Default スイッチにはマクロは適用されません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines スイッチからマクロを削除するには、マクロコマンドの **no** 形式を入力します。

macro auto config *macro-name* コマンドを入力すると、すべてのマクロパラメータの値を入力するよう要求されます。

macro-name および *parameters* を入力する場合は、正確なテキスト文字列を使用します。エントリは大文字と小文字が区別されます。

ユーザ定義の値は、**show macro auto** または **show running-config** コマンドの出力でのみ表示されます。

Cisco IOS シェルのスクリプト機能を使用してパラメータを設定することもできます。例については、「Configuring Auto Smartports and Static Smartports Macros」の章の「Configuring and Applying Global Macros」セクションを参照してください。

macro auto control

検出方法、デバイスタイプ、またはトリガー（イベントトリガーコントロールとも呼ばれる）に基づいてスイッチに Auto Smartport マクロを適用するタイミングを指定するには、インターフェイス コンフィギュレーション モードで **macro auto control** コマンドを使用します。トリガーとマクロのマッピングをディセーブルにするには、このコマンドの **no** 形式を使用します。これで、スイッチはイベント トリガーに基づいてマクロを適用しなくなります。

```
macro auto control {detection [cdp] [lldp] [mac-address]} device [ip-camera] [media-player] [phone]
[lightweight-ap] [access-point] [router] [switch] | trigger [last-resort]}
no macro auto control {detection [cdp] [lldp] [mac-address]} device [ip-camera] [media-player]
[phone] [lightweight-ap] [access-point] [router] [switch] | trigger [last-resort]}
```

Syntax Description

detection [cdp] [lldp] [mac-address]

detection: 次の中の 1 つ以上を、イベントトリガーとして設定します。

- （任意） **cdp:** CDP メッセージ
- （任意） **lldp:** LLDP メッセージ
- （任意） **mac-address:** ユーザ定義の MAC アドレスグループ

device [access-point] [ip-camera] [lightweight-ap] [media-player] [phone] [router] [switch]

device: 次の 1 つ以上のデバイスを、イベント トリガーとして設定します。

- （任意） **access-point:** Autonomous アクセスポイント
- （任意） **ip-camera:** Cisco IP ビデオ監視カメラ
- （任意） **lightweight-ap:** 中央管理型アクセスポイント
- （任意） **media-player:** デジタルメディアプレーヤー
- （任意） **phone:** Cisco IP 電話
- （任意） **router:** Cisco ルータ
- （任意） **switch:** Cisco スイッチ

trigger [last-resort]

trigger: 特定のイベント トリガーを設定します。

- (任意) **last-resort:** ラストリゾートトリガー

Command Default

スイッチは、イベント トリガーとしてデバイス タイプを使用します。スイッチがデバイス タイプを決定できない場合は、MAC アドレス グループ、MAB メッセージ、802.1X 認証メッセージ、および LLDP メッセージをランダムな順序で使用します。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

イベント トリガーを設定しなかった場合、スイッチはイベント トリガーとしてデバイス タイプを使用します。スイッチがデバイス タイプを決定できない場合は、MAC アドレス グループ、MAB メッセージ、802.1X 認証メッセージ、および LLDP メッセージをランダムな順序で使用します。マクロがインターフェイスに適用されていることを確認するには、ユーザ EXEC モードで **show macro auto interface** コマンドを使用します。

例

次に、イベントトリガーとして LLDP メッセージおよび MAC アドレスグループを設定する例を示します。

```
Device(config)# interface gigabitethernet 5/0/2
Device(config-if)# macro auto control detection lldp mac-address
Device(config-if)# exit
Device(config)# end
```

次に、イベントトリガーとしてアクセスポイント、ビデオ監視カメラ、デジタルメディアプレーヤーを設定する例を示します。



Note

スイッチは、アクセスポイント、ビデオサーベイランスカメラ、またはデジタルメディアプレーヤーを検出した場合のみ組み込みマクロを適用します。

```
Device(config)# interface gigabitethernet 5/0/1
Device(config-if)# macro auto control device access-point ip-camera media-player
Device(config-if)# exit
Device(config)# end
```

macro auto execute

組み込みマクロのデフォルト値を置き換えて、イベントトリガーから組み込みマクロ、またはユーザ定義マクロへのマッピングを設定するには、グローバルコンフィギュレーションモードで **macro auto execute** コマンドを使用します。

```
macro auto execute event trigger {builtin built-in macro | remote url} {parameter=value} {function contents}
```

```
no macro auto execute event trigger {builtin built-in macro | remote url} {parameter=value} {function contents}
```

Syntax Description

event trigger

イベント トリガーから組み込みマクロへのマッピングを定義します。

event trigger に次の値を指定します。

- CISCO_CUSTOM_EVENT
- CISCO_DMP_EVENT
- CISCO_IPVSC_EVENT
- CISCO_LAST_RESORT_EVENT
- CISCO_PHONE_EVENT
- CISCO_ROUTER_EVENT
- CISCO_SWITCH_EVENT
- CISCO_WIRELESS_AP_EVENT
- CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
- **WORD:** MAC アドレスグループなどのユーザ定義イベントトリガーを適用します。

builtin <i>built-in macro name</i>	<p>(任意) builtin built-in macro name に次の値を指定します。</p> <ul style="list-style-type: none"> • CISCO_AP_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。 • CISCO_DMP_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。 • CISCO_IPVSC_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。 • CISCO_LWAP_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。 • CISCO_PHONE_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 および VOICE_VLAN=2 を指定します。 • CISCO_ROUTER_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。 • CISCO_SWITCH_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。
<i>parameter=value</i>	<p>(任意) <i>parameter=value</i>: <i>bultin-macro name</i> に示されたパラメータ値のデフォルト値 (例: ACCESS_VLAN=1) を置き換えます。それぞれの名前と値のペアをスペースで区切る形式で新しい値を入力します (例: [<i><name1>=<value1> <name2>=<value2>...</i>]) 。</p>
<i>{function contents}</i>	<p>(任意) <i>{function contents}</i>: トリガーに関連付けるユーザ定義のマクロを指定します。マクロの内容は、波カッコで囲んで入力します。左波カッコで Cisco IOS シェルコマンドを開始し、右波カッコでコマンドのグループ化を終了します。</p>

remote url (任意) リモート サーバの場所を次のように指定します。

- スタンドアロンスイッチ上またはスタックのアクティブスイッチ上のローカルフラッシュファイルシステムの構文: **flash**:
スタックメンバ上のローカルフラッシュファイルシステムの構文:
flash member number:
FTP の構文:
ftp:[[/username[:password]@location]/directory]/filename
HTTP サーバの構文:
http://[[username:password]@]{hostname | host-ip}[/directory]/filename
セキュア HTTP サーバの構文:
https://[[username:password]@]{hostname | host-ip}[/directory]/filename
NVRAM の構文:
nvrाम:[[/username:password]@]/[directory]/filename
リモート コピー プロトコル (RCP) の構文:
rcp:[[/username@location]/directory]/filename
Secure Copy Protocol (SCP) の構文:
scp:[[/username@location]/directory]/filename
TFTP の構文:
tftp:[[/location]/directory]/filename

Command Default	なし	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 組み込みマクロのデフォルト値をスイッチに固有の値で置き換えるには、**macro auto execute** コマンドを使用します。

イベント トリガーから組み込みマクロへのマッピングは、スイッチで自動的に実行されます。組み込みマクロはシステム定義のマクロであり、ソフトウェア イメージに含まれています。Cisco IOS シェルのスクリプト機能を使用してユーザ定義のマクロを作成することもできます。

グローバル コンフィギュレーション モードで **shell trigger** コマンドを使用すると、新しいイベントトリガーを作成できます。ユーザ定義のトリガーおよびマクロの内容を表示するには、特権 EXEC で **show shell triggers** コマンドを使用します。

Cisco Discovery Protocol (CDP) も Link Layer Discovery Protocol (LLDP) もサポートしていないデバイスのイベントトリガーを作成するには、グローバル コンフィギュレーション モードで **macro auto mac-address-group** コマンドを使用します。

リモートマクロ機能を使用して、指定ネットワーク スイッチにより使用される中央の場所にマクロを保存できます。これにより、複数のスイッチで使用するためにマクロ ファイルを保持し、更新することが可能になります。リモートサーバの場所およびマクロのパス情報を設定するには、**remote url** を使用します。保存するマクロ ファイルのファイル名拡張子に特別な要件はありません。

Auto Smartports マクロおよびアンチマクロ（アンチマクロは、リンク ダウンが発生した場合に適用済のマクロによって削除される部分です）には、次の注意事項と制限事項があります。

- 組み込みマクロは削除または変更できます。ただし、ユーザ定義のマクロを同じ名前で作成すると、組み込みマクロを無効にすることができます。元の組み込みマクロを復元するには、ユーザ定義のマクロを削除します。
- **macro auto device** コマンドと **macro auto execute** コマンドの両方をイネーブルにした場合は、最後に実行したコマンドで指定したパラメータがスイッチに適用されます。スイッチ上でアクティブにできるコマンドは片方だけです。
- マクロを適用した場合のシステム競合を回避するには、802.1X 認証以外のポート認証をすべて削除します。
- スイッチ上で Auto SmartPort をイネーブルにする場合は、ポートセキュリティは設定しないでください。
- 元の設定とマクロが競合した場合は、マクロが元のいくつかのコンフィギュレーション コマンドに適用されないか、またはアンチマクロでこれらのコマンドが削除されません（アンチマクロは適用済みのマクロの一部で、リンクダウンイベントのときにマクロを削除します）。
- たとえば、802.1X 認証がイネーブルになっている場合は、**switchport-mode access** 設定を削除できません。この場合は、**switchport-mode** 設定を削除する前に 802.1X 認証を削除する必要があります。
- Auto SmartPort マクロを適用する場合は、ポートを EtherChannel のメンバにはできません。
- 組み込みマクロのデフォルトのデータ VLAN は VLAN 1 です。デフォルトの音声 VLAN は VLAN 2 です。スイッチが異なるアクセス、ネイティブ、または音声 VLAN を使用する場合は、**macro auto device** または **macro auto execute** コマンドを使用して値を設定します。
- 802.1X 認証または MAC 認証バイパス (MAB) では、他社製のデバイスを検出するために、RADIUS サーバがシスコの属性と値のペア **auto-smart-port=event trigger** をサポートするように設定します。
- スイッチが Auto SmartPort マクロをサポートするのは、デバイスに直接接続されている場合だけです。ハブなどの複数のデバイス接続はサポートされていません。
- ポート上で認証がイネーブルになっている場合は、スイッチは、認証が失敗した場合の MAC アドレス トリガーを無視します。
- マクロ内と対応するアンチマクロ内では、CLI コマンドの順序が異なる場合があります。

例

次の例では、Cisco スイッチと Cisco IP Phone をスイッチへ接続するために、2つの組み込みマクロを使用する方法を示します。次の例では、トランクインターフェイス用にデフォルトの音声 VLAN、アクセス VLAN、およびネイティブ VLAN を変更します。

```
Device(config)# !!! the next command modifies the access and voice vlans
Device(config)# !!! for the built in Cisco IP phone auto smartport macro
Device(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Device(config)# !!! the next command modifies the Native vlan used for inter switch trunks
Device(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Device(config)# !!! the next command enables auto smart ports globally
Device(config)# macro auto global processing
Device(config)# exit
Device# !!! here is the running configuration of the interface connected
Device# !!! to another Cisco Switch after the Macro is applied
Device# show running-config interface gigabitethernet1/0/1
Building configuration...

Current configuration : 284 bytes
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 macro description CISCO_SWITCH_EVENT
end
```

次の例では、メディアプレーヤーと呼ばれるユーザ定義イベントトリガーをユーザ定義マクロにマッピングする方法を示します。

1. 802.1X または MAB に対応したスイッチポートにメディアプレーヤーを接続します。
2. RADIUS サーバ上で、属性と値のペアを auto-smart-port=DMP_EVENT に設定します。
3. スイッチ上で、イベントトリガー DMP_EVENT を作成し、ユーザ定義マクロ コマンドを入力します。
4. スイッチは、RADIUS サーバからの attribute-value pair=DMP_EVENT 応答を受け入れ、このイベントトリガーに関連付けられたマクロを適用します。

```
Device(config)# shell trigger DMP_EVENT mediaplayer
Device(config)# macro auto execute DMP_EVENT {
if [[ $LINKUP == YES ]]; then
conf t
 interface $INTERFACE
 macro description $TRIGGER
```

```

switchport access vlan 1
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
spanning-tree portfast
spanning-tree bpduguard enable
exit
fi
if [[ $LINKUP == NO ]]; then
conf t
interface $INTERFACE
    no macro description $TRIGGER
    no switchport access vlan 1
    if [[ $AUTH_ENABLED == NO ]]; then
        no switchport mode access
    fi
    no switchport port-security
    no switchport port-security maximum 1
    no switchport port-security violation restrict
    no switchport port-security aging time 2
    no switchport port-security aging type inactivity
    no spanning-tree portfast
    no spanning-tree bpduguard enable
    exit
fi

```

Table 13: サポートされている *Cisco IOS* シェルのキーワード

コマンド	説明
{	コマンドのグループ化を開始します。
}	コマンドのグループ化を終了します。
[[条件構成体として使用します。
]]	条件構成体として使用します。
else	条件構成体として使用します。
==	条件構成体として使用します。
fi	条件構成体として使用します。
if	条件構成体として使用します。
then	条件構成体として使用します。
-z	条件構成体として使用します。
\$	\$ 文字で始まる変数は、パラメータ値で置換されます。

コマンド	説明
#	# 文字を使用して、コメント テキストを入力します。

Table 14: サポートされていない *Cisco IOS* シェルの予約済キーワード

コマンド	説明
	パイプライン
case	条件構成体
esac	条件構成体
for	ループ構成体
機能	シェル関数
in	条件構成体
select	条件構成体
time	パイプライン
until	ループ構成体
while	ループ構成体

macro auto global control

デバイスタイプまたはトリガー（イベントトリガーコントロールとも呼ばれる）に基づいてスイッチに Auto Smartport マクロを適用するタイミングを指定するには、グローバル コンフィギュレーション モードで **macro auto global control** コマンドを使用します。トリガーとマクロのマッピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
macro auto global control {detection [cdp] [lldp][mac-address] | device [access-point] [ip-camera]
[lightweight-ap] [media-player] [phone] [router] [switch] | trigger [last-resort]}
no macro auto global control {detection [cdp] [lldp] [mac-address] | device [access-point] [ip-camera]
[lightweight-ap] [media-player] [phone] [router] [switch] | trigger [last-resort]}
```

Syntax Description

detection [cdp] [lldp] [mac-address]

detection: 次の中の 1 つ以上を、イベントトリガーとして設定します。

- (任意) **cdp:** CDP メッセージ
- (任意) **lldp:** LLDP メッセージ
- (任意) **mac-address:** ユーザ定義の MAC アドレスグループ

device [access-point] [ip-camera] [lightweight-ap] [media-player] [phone] [router] [switch]

device: 次の 1 つ以上のデバイスを、イベントトリガーとして設定します。

- (任意) **access-point:** Autonomous アクセスポイント
- (任意) **ip-camera:** Cisco IP ビデオ監視カメラ
- (任意) **lightweight-ap:** 中央管理型アクセスポイント
- (任意) **media-player:** デジタルメディアプレーヤー
- (任意) **phone:** Cisco IP 電話
- (任意) **router:** Cisco ルータ
- (任意) **switch:** Cisco スイッチ

trigger [last-resort]

trigger: 特定のイベントトリガーを設定します。

- (任意) **last-resort:** ラストリゾートトリガー

Command Default

スイッチは、イベント トリガーとしてデバイス タイプを使用します。スイッチがデバイス タイプを決定できない場合は、MAC アドレス グループ、MAB メッセージ、802.1X 認証メッセージ、および LLDP メッセージをランダムな順序で使用します。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

イベント トリガーを設定しなかった場合、スイッチはイベント トリガーとしてデバイス タイプを使用します。スイッチがデバイス タイプを決定できない場合は、MAC アドレス グループ、MAB メッセージ、802.1X 認証メッセージ、および LLDP メッセージをランダムな順序で使用します。マクロがスイッチに適用されていることを確認するには、ユーザ EXEC モードで **show macro auto global** コマンドを使用します。

例

次に、イベントトリガーとして CDP メッセージ、LLDP メッセージ、および MAC アドレスグループを設定する例を示します。

```
Device(config)# macro auto global control detection cdp lldp mac-address
Device(config)# end
```

次に、Autonomous アクセスポイント、中央管理型アクセスポイント、および IP 電話を設定する例を示します。

```
Device(config)# macro auto global control device access-point lightweight-ap phone
Device(config)# end
```

macro auto global processing

スイッチ上で Auto SmartPort マクロをイネーブルにするには、グローバル コンフィギュレーション モードで **macro auto global processing** コマンドを使用します。マクロをディセーブルにするには、このコマンドの **no** 形式を使用します。

macro auto global processing

no macro auto global processing

Command Default Auto Smartports がディセーブルになっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines スイッチ上でマクロをグローバルにイネーブルにするには、**macro auto global processing** コマンドを使用します。特定のポート上でマクロをディセーブルにするには、インターフェイスモードで **no macro auto processing** コマンドを使用します。

802.1X または MAB 認証を使用している場合は、シスコの属性と値のペア **auto-smart-port=event trigger** をサポートするように RADIUS サーバを設定する必要があります。認証が失敗した場合は、マクロは適用されません。802.1X または MAB 認証がインターフェイスで失敗すると、スイッチはフォールバック CDP イベント トリガーを使用しません。

CDP で識別されるデバイスが複数の機能をアドバタイズする場合、スイッチは、最初にスイッチ、次にルータという順序で機能を選択します。

マクロがインターフェイスに適用されていることを確認するには、特権 EXEC モードで **show macro auto interface** コマンドを使用します。

例

次の例では、スイッチで Auto SmartPort をイネーブルにする方法、および特定のインターフェイスでこの機能をディセーブルにする方法を示します。

```
Device(config)# macro auto global processing
Device(config)# interface gigabitethernet 0/1
Device(config-if)# no macro auto processing
Device(config-if)# exit
Device(config)#
```

macro auto mac-address-group

Cisco Discovery Protocol (CDP) または Link Layer Discover Protocol (LLDP) をサポートしていないデバイスのイベントトリガーを作成するには、グローバル コンフィギュレーション モードで **macro auto mac-address-group** コマンドを使用します。グループを削除するには、このコマンドの **no** 形式を使用します。

macro auto mac-address-group *name* {**mac-address list** *list* | **oui** {**list** *list* | **range** *start-value size number*}}
no macro auto mac-address-group *name* {**mac-address list** *list* | **oui** {**list** *list* | **range** *start-value size number*}}

Syntax Description

<i>name</i>	グループ名を指定します。
ui	(任意) Operationally Unique Identifier (OUI) の list または range を指定します。 <ul style="list-style-type: none"> • list: OUI リストを、スペースで区切った 16 進形式で入力します。 • range: OUI の開始値を 16 進数で入力します (<i>start-value</i>) 。 • size: 連続したアドレスリストを作成するための range の長さ (<i>number</i>) を 1 ~ 5 で入力します。
mac-address list <i>list</i>	(任意) スペースで区切った MAC アドレスのリストを設定します。

Command Default

グループは定義されていません。

Command Modes

グループ コンフィギュレーション (config-addr-grp-mac)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

CDP または LLDP をサポートしていないデバイスのイベントトリガーを作成するには、**macro auto mac-address-group** コマンドを使用します。**macro auto execute** コマンドを使用して、組み込みマクロまたはユーザ定義マクロをマッピングするには、MAC アドレスグループをトリガーとして使用します。リンクアップ時に、スイッチがデバイスタイプを検出し、指定されたマクロを適用します。

このスイッチは、最大 10 の MAC アドレス グループをサポートします。各グループは、最大 32 個の OUI と 32 個の MAC 設定済みアドレスを持つことができます。

例

次の例では、*address_trigger* という MAC アドレスグループ イベント トリガーを作成する方法、およびエントリを確認する方法を示します。

```
Device(config)# macro auto mac-address-group mac address_trigger
Device(config-addr-grp-mac)# mac-address list 2222.3333.3334 22.33.44 a.b.c
Device(config-addr-grp-mac)# oui list 455555 233244
Device(config-addr-grp-mac)# oui range 333333 size 2
Device(config-addr-grp-mac)# exit
Device(config)# end
Device# show running configuration
!
!macro auto mac-address-group address_trigger
  oui list 333334
  oui list 333333
  oui list 233244
  oui list 455555
  mac-address list 000A.000B.000C
  mac-address list 0022.0033.0044
  mac-address list 2222.3333.3334
!
<output truncated>
```

macro auto processing

インターフェイスで Auto SmartPort マクロをイネーブルにするには、インターフェイス コンフィギュレーションモードで **macro auto processing** コマンドを使用します。マクロをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

macro auto processing

no macro auto processing

Command Default Auto SmartPort はディセーブルになっています。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 特定のインターフェイスでマクロをイネーブルにするには、インターフェイス コンフィギュレーションモードで **macro auto processing** コマンドを使用します。特定のインターフェイスでマクロをディセーブルにするには、インターフェイス コンフィギュレーションモードで **no macro auto processing** コマンドを使用します。

Auto SmartPort マクロを適用する場合は、ポートを EtherChannel のメンバにはできません。EtherChannel を使用する際、**no macro auto processing** コマンドを使用して、EtherChannel インターフェイスの Auto SmartPort をディセーブルにします。EtherChannel インターフェイスが設定をメンバインターフェイスに適用します。

マクロがインターフェイスに適用されていることを確認するには、特権 EXEC モードで **show macro auto interface** コマンドを使用します。

例

次の例では、スイッチで Auto SmartPort をイネーブルにする方法、および特定のインターフェイスでこの機能をディセーブルにする方法を示します。

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# no macro auto processing
Device(config-if)# exit
Device(config)# macro auto global processing
```

macro auto sticky

リンクダウンイベントの後でもマクロがアクティブになる（マクロの永続性と呼ばれる）ように設定するには、グローバルコンフィギュレーションモードで **macro auto sticky** コマンドを使用します。マクロの永続性をディセーブルにするには、このコマンドの **no** 形式を使用します。

macro auto sticky
no macro auto sticky

Command Default	マクロの永続性はディセーブルになっています。	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	リンクダウンイベント後もマクロがアクティブになるよう、 macro auto sticky コマンドを使用します。	

例

次の例では、インターフェイス上でマクロの永続性をイネーブルにする方法を示します。

```
Device(config)# interface gigabitethernet 5/0/2
Device(config-if)# macro auto port sticky
Device(config-if)# exit
Device(config)# end
```

macro auto trigger

マクロ トリガー コンフィギュレーション モードを開始し、組み込みトリガーのないデバイスのトリガーを定義し、そのトリガーとデバイスまたはプロファイルに関連付けるには、グローバル コンフィギュレーション モードで **macro auto trigger** コマンドを使用します。ユーザ定義トリガーを削除するには、このコマンドの **no** 形式を使用します。

```
macro auto trigger trigger_name {device | exit | no | profile}
no macro auto trigger trigger_name {device | exit | no | profile}
```

Syntax Description		
<i>trigger_name</i>		デバイス タイプまたはプロファイル名に関連付けるトリガーを指定します。
device		名前付きトリガーにマッピングするデバイス名を指定します。
exit		デバイス グループ コンフィギュレーション モードを終了します。
no		設定されているデバイスをすべて削除します。
profile		名前付きトリガーにマッピングするプロファイル名を指定します。

Command Default ユーザ定義トリガーは設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デバイスが Device Classifier によって分類されているにもかかわらず、組み込みトリガーが定義されていない場合は、グローバル コンフィギュレーション モードで **macro auto trigger** コマンドを使用し、デバイス名またはプロファイル名に基づいてトリガーを定義します。このコマンドを入力すると、スイッチはマクロ トリガー コンフィギュレーション モードになり、**device**、**exit**、**no**、**profile** の各キーワードが表示されます。このモードで、トリガーにマッピングするデバイス名またはプロファイル名を指定できます。デバイス名とプロファイル名の両方にトリガーをマッピングする必要はありません。両方の名前にトリガーをマッピングすると、マクロ アプリケーションで、トリガーとプロファイル名のマッピングが優先されます。

ユーザ定義マクロを設定するときは、このコマンドを使用してトリガーを設定してください。カスタム マクロの設定ではトリガー名は必須です。

デバイスのプロファイルを作成したら、デバイスグループデータベースに、この文字列をそのまま追加する必要があります。

例

次に、組み込みトリガーのないメディアプレーヤーとともに使用するために、**mediaplayer-DMP** というプロファイルに対するユーザ定義トリガーを設定する方法を示します。

```
Device(config)# macro auto trigger DMP  
Device(config-macro-trigger) # profile mediaplayer-DMP  
Device(config-macro-trigger) # exit
```

macro description

インターフェイスにどのマクロが適用されるかについて説明を入力するには、インターフェイス コンフィギュレーション モードで **macro description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。このコマンドは Auto Smartport の稼働に必須です。

macro description *text*
no macro description *text*

Syntax Description	description <i>text</i>	指定したインターフェイスに適用されたマクロについての説明を入力します。
Command Default	このコマンドにはデフォルト設定はありません。	
Command Modes	インターフェイス コンフィギュレーション (config-if)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines インターフェイスにコメントテキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。単一インターフェイスに複数のマクロを適用する場合、説明テキストは最後に適用したマクロのものになります。

設定を確認するには、特権 EXEC モードで **show parser macro description** コマンドを入力します。

例

次の例では、インターフェイスに説明を追加する方法を示します。

```
デバイス(config-if)# macro description duplex settings
```

macro global

スイッチにマクロを適用するか、またはスイッチ上でマクロを適用およびデバッグするには、グローバル コンフィギュレーション モードで **macro global** コマンドを使用します。

```
macro global {apply | trace} macro-name [parameter {value}][parameter {value}][parameter {value}]
parameter
```

Syntax Description		
apply		スイッチにマクロを適用します。
trace		スイッチにマクロを適用してマクロをデバッグします。
<i>macro-name</i>		マクロ名を指定します。
parameter <i>value</i>		(任意) そのスイッチに限定された一意のパラメータ値を指定します。最高3つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。

Command Default このコマンドにはデフォルト設定はありません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Note マクロ内の各コマンドの **no** バージョンを入力したときにだけ、スイッチで適用されたグローバルマクロ設定を削除できます。

インターフェイスにマクロを適用するには、**macro global apply macro-name** コマンドを使用します。

マクロを適用し、マクロをデバッグして構文エラーまたは設定エラーを判別するには、**macro global trace macro-name** コマンドを使用します。

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをスイッチに適用します。

一意の値の割り当てを必要とするマクロを作成する場合、**parameter value** キーワードを使用して、そのスイッチに固有の値を指定します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

一部のマクロには、パラメータ値が必要なキーワードが含まれます。**macro global apply macro-name ?** コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。

スイッチソフトウェアには、シスコデフォルト **Smartports** マクロが埋め込まれています。これらのマクロやコマンドは、ユーザ EXEC モードで **show parser macro** コマンドを使用して表示できます。

スイッチにシスコデフォルト **Smartports** マクロを適用するときは、次の注意事項に従ってください。

- スイッチ上のすべてのマクロを表示するには、**show parser macro** コマンドを使用します。特定のマクロの内容を表示するには、**show parser macro name macro-name** コマンドを使用します。
- \$ で始まるキーワードには、一意のパラメータ値が必要です。**parameter value** キーワードを使用して、必要な値をシスコデフォルトマクロに追加します。

シスコデフォルトマクロは \$ という文字を使用しているため、必須キーワードを識別するのに役立ちます。マクロを作成する場合、\$ という文字を使用したキーワードの定義には制限がありません。

マクロをスイッチに適用する場合、マクロ名が自動的にスイッチに追加されます。**show running-config** コマンドを使用すると、適用されたコマンドおよびマクロ名を表示できます。

例

macro auto execute コマンドを使用して新しいマクロを作成した後で、そのマクロをスイッチに適用できます。次の例では、**snmp** マクロを表示する方法、およびそのマクロを適用してホスト名をテストサーバに設定し、**IP precedence** 値を 7 に設定する方法を示します。

```
Device# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

-----
Device(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

マクロをデバッグするには、**macro global trace** コマンドを使用して、マクロをスイッチに適用したときのマクロの構文または設定エラーを判別できます。この例では、**ADDRESS** パラメータ値が入力されていません。**snmp-server host** コマンドが失敗しており、マクロの残りの部分がスイッチに適用されています。

```
Device(config)# macro global trace snmp VALUE 7
Applying command...`snmp-server enable traps port-security'
Applying command...`snmp-server enable traps linkup'
Applying command...`snmp-server enable traps linkdown'
Applying command...`snmp-server host'
%Error Unknown error.
Applying command...`snmp-server ip precedence 7'
```

macro global description

スイッチに適用されるマクロについての説明を入力するには、グローバル コンフィギュレーション モードで **macro global description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

macro global description *text*

no macro global description *text*

Syntax Description	description <i>text</i>	スイッチに適用されたマクロについての説明を入力します。
Command Default	このコマンドにはデフォルト設定はありません。	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines スイッチにコメントテキストまたはマクロ名を関連付けるには、**description** キーワードを使用します。複数のマクロがスイッチに適用されている場合、説明テキストは最後に適用されたマクロの説明になります。

設定を確認するには、特権 EXEC モードで **show parser macro description** コマンドを入力します。

例

次の例では、スイッチに説明を追加する方法を示します。

```
Device(config)# macro global description udd aggressive mode enabled
```

max-endpoints (COAP プロキシ コンフィギュレーション)

デバイスで学習できるエンドポイントの最大数を指定するには、COAP プロキシ コンフィギュレーション モードで **max-endpoints** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

max-endpoints *number*
no max-endpoints

Syntax Description	<i>number</i>	範囲は 1 ~ 500 です。
Command Default	デフォルトのエンドポイント数は 10 です。	
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	COAP プロキシ コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで coap proxy コマンドを入力します。	

例

次に、デバイスで学習できるエンドポイントの最大数を 12 に指定する例を示します。

```
Device(config)# coap proxy  
Device(config-coap-proxy)# max-endpoints 12
```

mdix auto

インターフェイスで Automatic Medium-Dependent Interface Crossover (Auto MDIX) 機能をイネーブルにするには、インターフェイス コンフィギュレーション モードで **mdix auto** コマンドを使用します。Auto MDIX をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdix auto
no mdix auto

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default Auto MDIX は、イネーブルです。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Auto MDIX がイネーブルな場合、インターフェイスは自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定します。

インターフェイスの Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度とデュプレックスも **auto** に設定する必要があります。

Auto MDIX が（速度とデュプレックスの自動ネゴシエーションとともに）接続するインターフェイスの一方または両方でイネーブルの場合は、ケーブルタイプ（ストレートまたはクロス）が不正でもリンクがアップします。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mbps インターフェイス上および 10/100/1000BASE-T/TX Small Form-Factor Pluggable (SFP) モジュール インターフェイス上でサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

インターフェイスの Auto-MDIX の動作ステートを確認するには、**show controllers ethernet-controller interface-id phy** 特権 EXEC コマンドを入力します。

次の例では、ポートの Auto MDIX を有効にする方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto
Device(config-if)# duplex auto
Device(config-if)# mdix auto
Device(config-if)# end
```

monitoring

すべての光トランシーバのモニタリングを有効にし、トランシーバのモニタリング期間を指定するには、トランシーバタイプ コンフィギュレーション モードで **monitoring** コマンドを使用します。モニタリングを無効にするには、このコマンドの **no** 形式を使用します。

monitoring [*interval seconds*]
no monitoring [*interval*]

Syntax Description	<p>interval <i>seconds</i></p> <p>(任意) 光トランシーバをモニタリングする時間間隔を指定します。範囲は 300 ~ 3600 秒で、デフォルト間隔時間は 600 秒です。</p>
---------------------------	--

Command Default 間隔時間は 600 秒です。

Command Modes トランシーバタイプ コンフィギュレーション (config-xcvr-type)

Command History	<table border="1"> <tr> <th>リリース</th> <th>変更内容</th> </tr> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines **monitoring** コマンドを設定するには、デジタル オプティカル モニタリング (DOM) 機能およびトランシーバモジュールの互換性情報が必要です。[互換性マトリックス](#)を参照して、ギガビットイーサネットトランシーバモジュールをサポートするシスコのプラットフォームと最小必須ソフトウェアバージョンのリストを取得します。

ギガビットイーサネットトランシーバは、IEEE 802.3-2008 標準で定義されているように、ギガビット/秒のレートでイーサネットフレームを送受信します。シスコのギガビットイーサネットトランシーバモジュールは、シスコのすべてのスイッチングおよびルーティングプラットフォームでイーサネットアプリケーションをサポートします。これらの着脱可能なトランシーバは、データセンター、キャンパス、メトロポリタンエリアのアクセスおよびリングネットワーク、およびストレージエリアネットワークでの導入に便利でコスト効率の高いソリューションを提供します。

interval キーワードを使用すると、デフォルトのポーリング間隔を変更できます。たとえば、間隔を 1500 秒に設定すると、ポーリングは 1500 秒ごとに行われます。ポーリング期間中、光トランシーバの `entSensorStatus` は [Unavailable] に設定され、ポーリングが終了すると `entSensorStatus` に実際のステータスが表示されます。

Examples

次に、光トランシーバのモニタリングを有効にし、モニタリングの間隔時間を 1500 秒に設定する例を示します。

```
Device# configure terminal
Device(config)# transceiver type all
Device(config-xcvr-type)# monitoring interval 1500
```

次に、すべてのトランシーバタイプのモニタリングをディセーブルにする例を示します。

```
Device(config-xcvr-type)# no monitoring
```

Related Commands

Command	Description
transceiver type all	すべてのトランシーバのモニタリングを有効にします。

network-policy

インターフェイスにネットワークポリシープロファイルを適用するには、インターフェイスコンフィギュレーションモードで **network-policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

network-policy *profile-number*
no network-policy

Syntax Description	<i>profile-number</i> インターフェイスに適用するネットワークポリシープロファイル番号	
Command Default	ネットワークポリシープロファイルは適用されません。	
Command Modes	インターフェイス コンフィギュレーション (config-if)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines インターフェイスにプロファイルを適用するには、**network-policy** *profile number* インターフェイスコンフィギュレーションコマンドを使用します。

最初にネットワークポリシープロファイルを設定する場合、インターフェイスに **switchport voice vlan** コマンドを適用できません。ただし、**switchport voice vlan** *vlan-id* がすでにインターフェイス上に設定されている場合、ネットワークポリシープロファイルをインターフェイス上に適用できます。その後、インターフェイスは、適用された音声または音声シグナリング VLAN ネットワークポリシープロファイルを使用します。

次の例では、インターフェイスにネットワークポリシープロファイル 60 を適用する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# network-policy 60
```

network-policy profile (グローバル コンフィギュレーション)

ネットワークポリシー プロファイルを作成し、ネットワークポリシー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **network-policy profile** コマンドを使用します。ポリシーを削除して、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

network-policy profile *profile-number*
no network-policy profile *profile-number*

Syntax Description	<i>profile-number</i> ネットワークポリシー プロファイル番号。指定できる範囲は 1 ~ 4294967295 です。				
Command Default	ネットワークポリシー プロファイルは定義されていません。				
Command Modes	グローバル コンフィギュレーション (config)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードを開始するには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service (CoS)、Diffserv コードポイント (DSCP) の値、およびタギング モードを指定することで、音声および音声シグナリング用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) の network-policy Time Length Value (TLV) に含まれます。

次の例では、ネットワークポリシー プロファイル 60 を作成する方法を示します。

```
Device(config)# network-policy profile 60
Device(config-network-policy)#
```

port-dtls (COAP プロキシ コンフィギュレーション)

Datagram Transport Layer Security (DTLS) のポートを設定するには、COAP プロキシ コンフィギュレーションモードで **port-dtls** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-dtls *number*
no port-dtls

Syntax Description	<i>number</i>	範囲は 1 ~ 65000 です。
Command Default	デフォルトのポートは 5683 です。	
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	COAP プロキシ コンフィギュレーションモードにアクセスするには、グローバル コンフィギュレーションモードで coap proxy コマンドを入力します。	

例

次に、DTLS のポートを設定する例を示します。

```
Device(config)# coap proxy
Device(config-coap-proxy)# port-dtls 5899
```

port-unsecure (COAP プロキシ コンフィギュレーション)

ポートを設定するには、COAP プロキシ コンフィギュレーション モードで **port-unsecure** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-unsecure *number*
no port-dtls

Syntax Description	<i>number</i>	範囲は 1 ~ 65000 です。
Command Default	デフォルトのポートは 5683 です。	
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	COAP プロキシ コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで coap proxy コマンドを入力します。	

例

次に、ポートを設定する例を示します。

```
Device(config)# coap proxy
Device(config-coap-proxy)# port-unsecure 5899
```

power-priority

電源スタックのスイッチと高プライオリティおよび低プライオリティ PoE ポートに対して、Cisco StackPower の電源プライオリティ値を設定するには、スイッチスタック電源コンフィギュレーション モードで **power-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
power-priority {high value | low value | switch value}
no power-priority {high | low | switch}
```

Syntax Description

high value	ポートの電力プライオリティを高プライオリティポートとして設定します。値は 1～27 です。1 が最高のプライオリティです。 high の値は、低プライオリティポートに設定する値よりも小さく、スイッチに設定する値よりも大きくする必要があります。
low value	ポートの電力プライオリティを低プライオリティポートとして設定します。範囲は 1～27 です。 low の値は、高プライオリティポートおよびスイッチに設定された値よりも大きくする必要があります。
switch value	スイッチの電力プライオリティを設定します。範囲は 1～27 です。 switch の値は、低プライオリティポートおよび高プライオリティポートに設定された値よりも小さくする必要があります。

Command Default

値が設定されていない場合、電源スタックでは、デフォルトプライオリティがランダムに決定されます。

デフォルトの範囲は、スイッチで 1～9、高プライオリティポートで 10～18、低プライオリティポートで 19～27 です。

非 PoE スイッチでは、（ポートプライオリティの）高い値と低い値は、影響がありません。

Command Modes

スイッチスタック電源コンフィギュレーション (config-stack)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スイッチスタック電源コンフィギュレーション モードにアクセスするには、**stack-power switch switch-number** グローバルコンフィギュレーション コマンドを入力します。

Cisco StackPower の電源プライオリティ値によって、電源が失われ、負荷制限が発生した場合のスイッチとポートのシャットダウンの順序が決定されます。プライオリティ値は 1～27 です。最も高い数が最初にシャットダウンされます。

各スイッチ、その高プライオリティポート、および低プライオリティポートでは、異なるプライオリティ値を設定して、電源が失われている間に一度にシャットダウンされる装置数を制限することを推奨します。同じ電源スタックの異なるスイッチに同じプライオリティ値を設定しようとすると、設定は許可されますが、警告メッセージが表示されます。



Note このコマンドは、IP Base または IP Services フィーチャ セットが実行されているスイッチ スタックでのみ使用できます。

Examples

次に、電源スタックの switch 1 の電源プライオリティを 7 に、高プライオリティ ポートを 11 に、低プライオリティ ポートを 20 に設定する例を示します。

```
Device(config)# stack-power switch 1
Device(config-switch-stackpower)# stack-id power_stack_a
Device(config-switch-stackpower)# power-priority high 11
Device(config-switch-stackpower)# power-priority low 20
Device(config-switch-stackpower)# power-priority switch 7
Device(config-switch-stackpower)# exit
```

power inline

Power over Ethernet (PoE) ポートで電源管理モードを設定するには、インターフェイス コンフィギュレーション モードで **power inline** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
power inline {auto [max max-wattage] | never | port priority {high | low} | static [max max-wattage]}
no power inline {auto | never | port priority {high | low} | static [max max-wattage]}
```

Syntax Description		
auto		受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。割り当ては、検出された順序で行われます。
max max-wattage		(任意) ポートに供給される電力を制限します。指定できる範囲は 4000 ~ 30000 mW です。値を指定しない場合は、最大電力が供給されます。
never		装置の検出とポートへの電力供給をディセーブルにします。
port		ポートの電源プライオリティを設定します。デフォルトの優先度は [Low] です。
priority {high low}		ポートの電源プライオリティを設定します。電源に障害が発生した場合には、低プライオリティとして設定されているポートが最初にオフになり、高プライオリティとして設定されたポートは最後にオフになります。デフォルトの優先度は [Low] です。

static

受電装置の検出をイネーブルにします。スイッチが受電デバイスを検出する前に、ポートへの電力を事前に割り当てます（確保します）。このアクションによって、インターフェイスに接続されたデバイスで十分な電力を受け取ることができます。

Command Default

デフォルトは **auto**（イネーブル）です。
 最大ワット数は、30,000 mW です。
 デフォルトのポート プライオリティは低です。

Command Default

インターフェイス コンフィギュレーション（config-if）

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

このコマンドは、PoE 対応ポートだけでサポートされています。PoE がサポートされていないポートでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline auto
                        ^
% Invalid input detected at '^' marker.
```

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全ポートでサポートされます。

max max-wattage オプションを使用して、受電デバイスの電力が制限を超えないようにします。この設定によって、受電デバイスが最大ワット数より多い電力を要求する Cisco Discovery Protocol（CDP）メッセージを送信すると、スイッチはポートへ電力を供給しません。受電装置の IEEE クラスの最大値が最大ワット数を超えると、スイッチは装置に電力を供給しません。電力は、グローバル電力バジェットに送られます。



Note

power inline max max-wattage コマンドが 30 W 未満に設定されている場合、スイッチは Class 0 または Class 3 装置に電力を供給しません。

スイッチが受電デバイスへの電力供給を拒否する場合（受電デバイスが CDP メッセージを通じて制限を超えた電力を要求する場合、または IEEE クラスの最大値が最大ワット数を超えている場合）、PoE ポートは **power-deny** ステートになります。スイッチはシステムメッセージを生成し、**show power inline** 特権 EXEC コマンド出力の Oper カラムに **power-deny** が表示されます。

ポートに高いプライオリティを与えるには、**power inline static maxmax-wattage** コマンドを使用します。スイッチは、auto モードに設定されたポートに電力を割り当てる前に、static モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティック ポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティック ポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電デバイスからの CDP メッセージによって調節されることはありません。電力が事前割り当てられているので、最大ワット数以下の電力を使用する受電デバイスは、スタティック ポートに接続されていれば電力が保証されます。ただし、受電デバイスの IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。CDP メッセージを通じて受電デバイスが最大ワット数を超えた量を要求していることをスイッチが認識すると、受電デバイスがシャットダウンします。

ポートが static モードの場合にスイッチが電力を事前割り当てできない場合（たとえば、電力バジェット全体がすでに別の自動ポートまたはスタティック ポートに割り当てられているなど）、次のメッセージが表示されます。Command rejected: power inline static: pwr not available。ポートの設定は、そのまま変更されません。

power inline auto または **power inline static** インターフェイス コンフィギュレーション コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定を使用して自動ネゴシエーションします。これは、受電デバイスであるかどうかに関係なく、接続された装置の電力要件を判別するのに必要です。電力要件が判別された後、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定に戻ります。

ポートにシスコ製の受電デバイスが接続されている場合は、**power inline never** コマンドでポートを設定しないでください。不正なリンクアップが生じ、ポートが errdisable ステートになる可能性があります。

power inline port priority {high | low} コマンドを使用して、PoE ポートの電源プライオリティを設定します。電力が不足した場合には、低いポート プライオリティでポートに接続されている受電デバイスが、まず、シャットダウンされます。

設定を確認するには、**show power inline EXEC** コマンドを入力します。

Examples

次の例では、スイッチ上で受電デバイスの検出をイネーブルにし、PoE ポートに自動的に電力を供給する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto
```

次の例では、Class 1 または Class 2 の受電デバイスを受け入れるように、スイッチ上で PoE ポートを設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、スイッチ上で PoE ポートへの電力供給を停止する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline never
```

次の例では、電源に障害が発生した場合に最後のポートの1つがシャットダウンされるよう、ポートのプライオリティを高に設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline port priority high
```

power inline police

受電デバイスでリアルタイム電力消費のポリシングをイネーブルにするには、インターフェイス コンフィギュレーションモードで **power inline police** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

power inline police [action {errdisable | log}]
no power inline police

Syntax Description	action errdisable	(任意) リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力をオフにするよう、デバイスを設定します。これがデフォルトのアクションになります。
	action log	(任意) リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、接続されているデバイスへの電力を供給しながら、デバイスが syslog メッセージを生成するように設定します。

Command Default 受電デバイスのリアルタイムの電力消費のポリシングは、ディセーブルです。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、Power of Ethernet (PoE) 対応ポートのみでサポートされています。PoEをサポートしていないデバイスまたはポートでこのコマンドを入力すると、エラーメッセージが表示されます。

スイッチスタックでは、このコマンドは、PoEおよびリアルタイム電力消費モニタリングをサポートしているスタックの全スイッチまたはポートでサポートされます。

リアルタイムの電力消費のポリシングがイネーブルである場合、受電デバイスが割り当てられた最大電力より多くの量を消費すると、デバイスが対処します。

PoEがイネーブルである場合、デバイスは受電デバイスのリアルタイムの電力消費を検知します。この機能は、パワー モニタリングまたはパワー センシングといわれます。また、デバイスはパワーポリシング機能を使用して消費電力をポリシングします。

パワーポリシングがイネーブルである場合、デバイスは次の順のいずれかの方式で PoE ポートのカットオフ電力として、これらの値の1つを使用します。

1. **power inline auto max max-wattage** インターフェイス コンフィギュレーション コマンドまたは **power inline static max max-wattage** インターフェイス コンフィギュレーション コマンドを入力したときにポート上で許可される電力を制限するユーザ定義の電力レベル。

2. デバイスでは、CDP パワーネゴシエーションまたは IEEE 分類および LLDP 電力ネゴシエーションを使用して、装置の消費使用量が自動的に設定されます。

カットオフ電力量の値を手動で設定しない場合、デバイスは、CDP 電力ネゴシエーションまたはデバイスの IEEE 分類と LLDP 電力ネゴシエーションを使用して自動的に値を決定します。CDP または LLDP がイネーブルでない場合は、デフォルト値の 30 W が適用されます。ただし、CDP または LLDP がない場合は、15400 ~ 30000 mW の値が CDP 要求または LLDP 要求だけに基づいて割り当てられるため、デバイスで 15.4 W を超える電力の消費がデバイスから許可されません。受電デバイスが CDP または LLDP のネゴシエーションなしに 15.4 W を超える電力を消費する場合、装置は最大電流 I_{max} の制限に違反し、最大値を超える電流が供給されるという I_{cut} 障害が発生する可能性があります。再び電源を入れるまで、ポートは障害状態のままになります。ポートで継続的に 15.4 W を超える電力が給電される場合、このサイクルが繰り返されます。

PoE+ ポートに接続されている受電デバイスが再起動し、電力 TLV で CDP パケットまたは LLDP パケットが送信される場合、デバイスは最初のパケットの電力ネゴシエーションプロトコルをロックし、その他のプロトコルからの電力要求に応答しません。たとえば、デバイスが CDP にロックされている場合、LLDP 要求を送信するデバイスに電力を供給しません。デバイスが CDP にロックされた後で CDP がディセーブルになった場合、デバイスは LLDP 電源要求に応答せず、アクセサリの電源がオンにならなくなります。この場合、受電デバイスを再起動する必要があります。

パワーポリシングがイネーブルである場合、デバイスはリアルタイムの電力消費を PoE ポートに割り当てられた最大電力と比較して、消費電力をポリシングします。装置が最大電力割り当て（またはカットオフ電力）を超える電力をポートで使用している場合、スイッチでは、ポートへの電力供給がオフにされるか、または装置に電力を供給しながら `syslog` メッセージが生成されて LED（ポート LED はオレンジ色に点滅）が更新されます。

- ポートへの電力供給をオフにして、ポートを `error-disabled` ステートとするようデバイスを設定するには、`power inline police` インターフェイス コンフィギュレーション コマンドを使用します。
- 装置に電力を供給しながら、`syslog` メッセージを生成するようデバイスを設定するには、`power inline police action log` コマンドを使用します。

`action log` キーワードを入力しない場合のデフォルトのアクションは、ポートのシャットダウン、ポートへの電力供給のオフ、およびポートを `PoE error-disabled` ステートに移行になります。PoE ポートを `error-disabled` ステートから自動的に回復するよう設定するには、`errdisable detect cause inline-power` グローバル コンフィギュレーション コマンドを使用して、PoE 原因に対する `error-disabled` 検出をイネーブルにして、`errdisable recovery cause inline-power interval interval` グローバル コンフィギュレーション コマンドを使用して、PoE `error-disabled` 原因の回復タイマーをイネーブルにします。



Caution ポリシングがディセーブルである場合、受電デバイスがポートに割り当てられた最大電力より多くの量を消費しても対処されないため、デバイスに悪影響を与える場合があります。

設定を確認するには、`show power inline police` 特権 EXEC コマンドを入力します。

Examples

次の例では、電力消費のポリシングをイネーブルにして、デバイスのPoEポートでsyslogメッセージを生成するようデバイスを設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# power inline police action log
```

power supply

スイッチの内部電源を設定および管理するには、特権 EXEC モードで **power supply** コマンドを使用します。

power supply *stack-member-number* **slot** {**A** | **B**} {**off** | **on**}

Syntax Description

<i>stack-member-number</i>	内部電源を設定するスタックメンバ番号。指定できる範囲は、スタック内のスイッチの数に応じて 1～9 です。 このパラメータは、スタック対応スイッチだけで使用できません。
slot	設定するスイッチの電源を選択します。
A	スロット A の電源を選択します。
B	スロット B の電源を選択します。 Note 電源スロット B は、スイッチの外側エッジに最も近いスロットです。
off	スイッチの電源をオフに設定します。
on	スイッチの電源をオンに設定します。

Command Default

スイッチの電源がオンになります。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

power supply コマンドは、スイッチまたはすべてのスイッチが同じプラットフォームであるスイッチスタックに適用されます。

同じプラットフォームスイッチを含むスイッチスタックでは、**slot** {**A** | **B**} **off** または **on** キーワードの入力前にスタックメンバを指定する必要があります。

デフォルト設定に戻すには、**power supply stack-member-number on** コマンドを使用します。

設定を確認するには、**show env power** 特権 EXEC コマンドを入力します。

Examples

次に、スロット A の電源装置をオフに設定する例を示します。

```
Device> power supply 2 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Device
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

次に、スロット A の電源装置をオンに設定する例を示します。

```
Device> power supply 1 slot B on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

次に、show env power コマンドの出力例を示します。

```
Device> show env power
SW  PID                Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  PWR-1RUC2-640WAC    DCB1705B05B OK           Good     Good     250/390
1B  Not Present
```

power supply autoLC shutdown

ラインカードの自動シャットダウン制御をイネーブルにするには、グローバルコンフィギュレーションモードでコマンドを使用します。**power supply autoLC shutdown** このコマンドはデフォルトでイネーブルになっており、ディセーブルにはできません。ディセーブルにしようとする、[AutoLC shutdown cannot be disabled] というメッセージが表示されます。

power supply autoLC shutdown
no power supply autoLC shutdown

Syntax Description	このコマンドには引数またはキーワードはありません。	
Command Default	ラインカードの自動シャットダウン制御はイネーブルになっています。	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、ラインカードで自動シャットダウンをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# power supply autoLC shutdown
```

resource directory (COAP プロキシ コンフィギュレーション)

スイッチが COAP クライアントとして動作できるユニキャストアップストリームリソースのディレクトリサーバを設定するには、COAP プロキシ コンフィギュレーションモードで **resource directory** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

resource directory コマンドを使用して、ipv4 または ipv6 のそれぞれについて、最大 5 つの IP リストを設定できます。

resource directory {ipv4 | ipv6}[ip-address]
no resource directory

Syntax Description	ipv4 <i>ip-address</i>	IPv4 アドレスを指定します。
	ipv6 <i>ip-address</i>	IPv6 アドレスを指定します。
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	COAP プロキシ コンフィギュレーションモードにアクセスするには、グローバル コンフィギュレーションモードで coap proxy コマンドを入力します。	

例

次に、スイッチが COAP クライアントとして動作できるユニキャストアップストリームリソースのディレクトリサーバを設定する例を示します。

```
Device(config)# coap proxy
Device(config-coap-proxy)# resource-directory ipv4 192.168.1.1
```

security (COAP プロキシ コンフィギュレーション)

CoAPセキュリティ機能を設定するには、COAPプロキシコンフィギュレーションモードで**security** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
security {none [ipv4 { ip-address ip-mask/prefix} | ipv6 { ip-address ip-mask/prefix} | list {ipv4-list-name
ipv6-list-name}] | dtls {[id-trustpoint {identity-trustpoint label}][verification-trustpoint {
verification-trustpoint}]} | [ipv4 { ip-address ip-mask/prefix} | ipv6 { ip-address ip-mask/prefix} | list
{ipv4-list-name ipv6-list-name}]}}
no security
```

Syntax Description	<p>none そのポートにセキュリティがないことを示します。</p> <p>Note 最大で5つのIPv4アドレスと5つのIPv6アドレスを関連付けることができます。</p> <hr/> <p>dtls DTLSセキュリティは、オプションであるRSAトラストポイントと検証トラストポイントを要します。1.1.0.0255.255.0.0検証トラストポイントがないと、通常の公開キー交換が行われます。</p> <p>Note 最大で5つのIPv4アドレスと5つのIPv6アドレスを関連付けることができます。</p>				
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	COAP プロキシ コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで coap proxy コマンドを入力します。				

例

次に、ポートをセキュリティなしに設定する例を示します。

```
Device(config)# coap proxy
Device(config-coap-proxy)# security none ipv4 1.1.0.0 255.255.0.0
```

shell trigger

イベントトリガーを作成するには、グローバル コンフィギュレーション モードで **shell trigger** コマンドを使用します。トリガーを削除するには、このコマンドの **no** 形式を使用します。

shell trigger *identifier description*

no shell trigger *identifier description*

Syntax Description	<i>identifier</i>	イベント トリガー ID を指定します。この ID を指定する場合は、文字間にスペースやハイフンを入れないでください。
	<i>description</i>	イベント トリガーの説明文を指定します。

Command Default	システム定義のイベント トリガー	
	<ul style="list-style-type: none"> • CISCO_DMP_EVENT • CISCO_IPVSC_AUTO_EVENT • CISCO_PHONE_EVENT • CISCO_SWITCH_EVENT • CISCO_ROUTER_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT 	

Command Modes	グローバル コンフィギュレーション (config)
----------------------	----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **macro auto device** および **macro auto execute** グローバル コンフィギュレーション コマンドで使用するためのユーザ定義イベントトリガーを作成するには、このコマンドを使用します。

IEEE 802.1X 認証を使用している場合にダイナミックデバイス検出に対応できるようにするには、シスコの属性と値のペア **auto-smart-port=event trigger** をサポートするように RADIUS 認証サーバを設定します。

例

次の例では、RADIUS_MAB_EVENT というユーザ定義のイベント トリガーを作成する方法を示します。

```
Device(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event  
Device(config)# end
```

show beacon all

デバイス上のビーコン LED のステータスを表示するには、特権 EXEC モードで **show beacon all** コマンドを使用します。

show beacon {rp {active | standby} | slot slot-number } |all}

Syntax Description	rp {active standby}	ビーコン LED のステータスを表示するアクティブまたはスタンバイのスイッチを指定します。
	slot slot-num	ビーコン LED のステータスを表示するスロットを指定します。
	all	すべてのビーコン LED のステータスを表示します。

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Command Default このコマンドには、デフォルト設定がありません。

Command Modes 特権 EXEC (#)

Usage Guidelines すべてのビーコン LED のステータスを確認するには、**show beacon all** コマンドを使用します。

show beacon all コマンドの出力例。

```
Device#show beacon all
Switch# Beacon Status
-----
*1          OFF
```

show beacon rp コマンドの出力例。

```
Device#show beacon rp active
Switch# Beacon Status
-----
*1          OFF
```

```
Device#show beacon slot 1
Switch# Beacon Status
-----
*1          OFF
```

show coap dtls endpoints

CoAPDTLS エンドポイントを表示するには、ユーザEXECモードまたは特権EXECモードで **show coap dtls endpoints** コマンドを使用します。

show coap dtls endpoints

Command Default

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)
 特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、CoAP DTLS エンドポイントを表示する例を示します。

```
Device# show coap dtls endpoints
#      Index StateString StateValue  Port IP
-----
```

show coap endpoints

CoAP エンドポイントを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show coap endpoints** コマンドを使用します。

show coap endpoints

Command Default

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、CoAP エンドポイントを表示する例を示します。

```
Device# show coap endpoints
List of all endpoints :

Code : D - Discovered , N - New
#      Status  Age(s)    LastWKC(s)    IP
-----
Endpoints - Total : 0 Discovered : 0 New : 0
```

show coap globals

CoAP のグローバル情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show coap globals** コマンドを使用します。

show coap globals

Command Default	このコマンドには引数またはキーワードはありません。	
Command Modes	ユーザ EXEC (>) 特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、**show coap globals** コマンドの出力例を示します。

次に、CoAP の設定を表示する例を示します。

```
Device# show coap dtls globals
Coap System Timer Values :
  Discovery   : 120 sec
  Cache Exp  : 5 sec
  Keep Alive  : 120 sec
  Client DB   : 5 sec
  Query Queue: 500 ms
  Ack delay   : 500 ms
  Timeout     : 5 sec
  Ageout      : 300 sec

Max Endpoints      : 10

Max DTLS Endpoints : 20
Resource Disc Mode : POST
```

show coap resources

CoAP リソースを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show coap resources** コマンドを使用します。

show coap resources

Command Default

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、CoAP リソースを表示する例を示します。

```
Device# show coap resources
Link format data =

</>
</cisco/flood>
</cisco/context>
</cisco/showtech>
</cisco/discover>
</cisco/sleep>
</cisco/lldp>
```

show coap stats

CoAP の統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show coap stats** コマンドを使用します。

show coap stats

Command Default

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、CoAP の統計情報を表示する例を示します。

```
Device# show coap stats
Coap Stats :
Endpoints   : 0
Requests    : 20
Ext Queries : 0
New Endpoints: 0
```

show coap version

CoAP のバージョンを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show coap version** コマンドを使用します。

show coap version

Command Default

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、CoAP のバージョンを表示する例を示します。

```
Device# show coap version
CoAP version 1.0.5
RFC 7252
```

show device classifier attached

スイッチに接続されているデバイスとそのプロパティを表示するには、ユーザ EXEC モードで **show device classifier attached** コマンドを使用します。

show device classifier attached [**detail** | **interface***interface_id* | **mac-address** *mac_address*]

Syntax Description	detail	
		詳細なデバイス分類子情報を表示します。
	interface <i>interface_id</i>	特定のインターフェイスに接続されたデバイスに関する情報を表示します。
	mac <i>mac_address</i>	指定したエンドポイントのデバイス情報を表示します。
Command Modes	ユーザ EXEC (>) 特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	このコマンドを使用して、スイッチに接続されているデバイスを表示します。デバイスの設定可能なパラメータを表示するには、特権 EXEC モードで show device classifier attached コマンドを使用します。	

例

次に、オプションのキーワードを指定せずに **show device classifier attached** コマンドを使用して、スイッチに接続されたデバイスを表示する例を示します。

```
Device# show device classifier attached
MAC_Address      Port_Id      Profile Name
=====
000a.b8c6.1e07   Gi1/0/2     Cisco-Device
001f.9e90.1250   Gi1/0/4     Cisco-AP-Aironet-1130
=====
```

次に、特権 EXEC モードでオプションの **mac-address** キーワードを指定して **show device classifier attached** コマンドを使用して、指定した MAC アドレスの接続デバイスに関するサマリー情報を表示する例を示します。

```
Device# show device classifier attached mac-address 001f.9e90.1250
MAC_Address      Port_Id      Profile Name
=====
```

```
001f.9e90.1250    Gi1/0/4    Cisco-AP-Aironet-1130
=====
```

次に、特権 EXEC モードでオプションの **mac-address** キーワードと **detail** キーワードを指定して **show device classifier attached** コマンドを使用して、指定した MAC アドレスの接続デバイスに関する詳細情報を表示する例を示します。

```
Device# show device classifier attached mac-address 001f.9e90.1250 detail
MAC_Address      Port_Id      Certainty Parent      ProfileType      Profile Name
  Device_Name
=====
001f.9e90.1250   Gi1/0/4      40         2             Built-in         Cisco-AP-Aironet-1130
  cisco AIR-LAP1131AG-E-K9
=====
```

次に、特権 EXEC モードでオプションの **interface** キーワードを指定して **show device classifier attached** コマンドを使用して、指定したインターフェイスに接続されたデバイスに関するサマリー情報を表示する例を示します。

```
Device# show device classifier attached interface gi 1/0/2
MAC_Address      Port_Id      Profile Name
=====
000a.b8c6.1e07   Gi1/0/2      Cisco-Device
=====
```

次に、特権 EXEC モードでオプションの **interface** キーワードと **detail** キーワードを指定して **show device classifier attached** コマンドを使用して、指定したインターフェイスに接続されたデバイスに関する詳細情報を表示する例を示します。

```
Device# show device classifier attached interface gi 1/0/2 detail
MAC_Address      Port_Id      Certainty Parent      ProfileType      Profile Name
  Device_Name
=====
000a.b8c6.1e07   Gi1/0/2      10         0             Default          Cisco-Device      cisco
WS-C2960-48TT-L
=====
```

show device classifier clients

スイッチのデバイス分類子機能を使用しているクライアントを表示するには、ユーザ EXEC モードで **show device classifier clients** コマンドを使用します。

show device classifier clients

Command Default

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デバイス分類子 (DC) は、この機能を使用するクライアントアプリケーション (Auto SmartPort など) をイネーブルにすると、デフォルトでイネーブルになります。スイッチの DC 機能を使用しているクライアントを表示するには、**show device classifier clients** コマンドを使用します。

いずれかのクライアントが DC を使用中の間は、**no device classifier** コマンドを使用して DC をディセーブルにすることはできません。クライアントが使用中の DC をディセーブルにしようとすると、エラー メッセージが表示されます。

例

次に、**show device classifier clients** コマンドを使用して、スイッチの DC を使用中のクライアントを表示する例を示します。

```
Device# show device classifier clients
Client Name
=====
Auto Smart Ports
```

This example shows the error message that appears when you attempt to disable DC while a client is using it:

```
Switch(config)# no device classifier
These subsystems should be disabled before disabling Device classifier
Auto Smart Ports
```

```
% Error - device classifier is not disabled
```

show device classifier profile type

デバイス分類子によって認識されているデバイスタイプをすべて表示するには、ユーザ EXEC モードで **show device classifier profile type** コマンドを使用します。

show device classifier profile type [table [built-in default] | string filter_string]

Syntax Description	table	built-in	default	filter string
	デバイス分類子を表形式で表示します。			
		組み込みデバイス テーブルのデバイス分類子情報を表示します。		
			デフォルトのデバイス テーブルのデバイス分類子情報を表示します。	
				フィルタに一致するデバイスの情報を表示します。

Command Modes	ユーザ EXEC (>) 特権 EXEC (#)
---------------	-----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、デバイス分類子エンジンで認識されているすべてのデバイスタイプを表示します。表示されるデバイスタイプの数、スイッチに保存されているプロファイルの数です。プロファイル数が非常に多いことがあるため、**filter** キーワードを使用してコマンド出力を制限します。

例

次に、特権 EXEC モードでオプションのキーワードを何も指定せずに **show device classifier profile type** コマンドを使用して、デバイス分類子によって認識されているデバイスを表示する例を示します。

```
Device# show device classifier profile type table
  Valid      Type      Profile Name      min Conf  ID
  =====  =====  =====
  Valid      Default   Apple-Device      10        0
  Valid      Default   Aruba-Device      10        1
  Valid      Default   Avaya-Device      10        2
  Valid      Default   Avaya-IP-Phone    20        3
  Valid      Default   BlackBerry         20        4
  Valid      Default   Cisco-Device      10        5
  Valid      Default   Cisco-IP-Phone    20        6
  Valid      Default   Cisco-IP-Phone-7902 70        7
```

show device classifier profile type

Valid	Default	Cisco-IP-Phone-7905	70	8
Valid	Default	Cisco-IP-Phone-7906	70	9
Valid	Default	Cisco-IP-Phone-7910	70	10
Valid	Default	Cisco-IP-Phone-7911	70	11
Valid	Default	Cisco-IP-Phone-7912	70	12
Valid	Default	Cisco-IP-Phone-7940	70	13
Valid	Default	Cisco-IP-Phone-7941	70	14
Valid	Default	Cisco-IP-Phone-7942	70	15
Valid	Default	Cisco-IP-Phone-7945	70	16
Valid	Default	Cisco-IP-Phone-7945G	70	17
Valid	Default	Cisco-IP-Phone-7960	70	18
Valid	Default	Cisco-IP-Phone-7961	70	19
Valid	Default	Cisco-IP-Phone-7962	70	20
Valid	Default	Cisco-IP-Phone-7965	70	21
Valid	Default	Cisco-IP-Phone-7970	70	22
Valid	Default	Cisco-IP-Phone-7971	70	23
Valid	Default	Cisco-IP-Phone-7975	70	24
Valid	Default	Cisco-IP-Phone-7985	70	25
Valid	Default	Cisco-IP-Phone-9971	70	26
Valid	Default	Cisco-WLC-2100-Series	40	27
Valid	Default	DLink-Device	10	28
Valid	Default	Enterasys-Device	10	29
Valid	Default	HP-Device	10	30
Valid	Default	HP-JetDirect-Printer	30	31
Valid	Default	Lexmark-Device	10	32
Valid	Default	Lexmark-Printer-E260dn	30	33
Valid	Default	Microsoft-Device	10	34
Valid	Default	Netgear-Device	10	35
Valid	Default	NintendoWII	10	36
Valid	Default	Nortel-Device	10	37
Valid	Default	Nortel-IP-Phone-2000-Series	20	38
Valid	Default	SonyPS3	10	39
Valid	Default	XBOX360	20	40
Valid	Default	Xerox-Device	10	41
Valid	Default	Xerox-Printer-Phaser3250	30	42
Valid	Default	Aruba-AP	20	43
Valid	Default	Cisco-Access-Point	10	44
Valid	Default	Cisco-IP-Conference-Station-7935	70	45
Valid	Default	Cisco-IP-Conference-Station-7936	70	46
Valid	Default	Cisco-IP-Conference-Station-7937	70	47
Valid	Default	DLink-DAP-1522	20	48
Valid	Default	Cisco-AP-Aironet-1130	30	49
Valid	Default	Cisco-AP-Aironet-1240	30	50
Valid	Default	Cisco-AP-Aironet-1250	30	51
Valid	Default	Cisco-AIR-LAP	25	52
Valid	Default	Cisco-AIR-LAP-1130	30	53
Valid	Default	Cisco-AIR-LAP-1240	50	54
Valid	Default	Cisco-AIR-LAP-1250	50	55
Valid	Default	Cisco-AIR-AP	25	56
Valid	Default	Cisco-AIR-AP-1130	30	57
Valid	Default	Cisco-AIR-AP-1240	50	58
Valid	Default	Cisco-AIR-AP-1250	50	59
Invalid	Default	Sun-Workstation	10	60
Valid	Default	Linksys-Device	20	61
Valid	Default	LinksysWAP54G-Device	30	62
Valid	Default	HTC-Device	10	63
Valid	Default	MotorolaMobile-Device	10	64
Valid	Default	VMWare-Device	10	65
Valid	Default	ISE-Appliance	10	66
Valid	Built-in	Cisco-Device	10	0
Valid	Built-in	Cisco-Router	10	1
Valid	Built-in	Router	10	2
Valid	Built-in	Cisco-IP-Camera	10	3
Valid	Built-in	Cisco-IP-Camera-2xxx	30	4

Valid	Built-in	Cisco-IP-Camera-2421	50	5
Valid	Built-in	Cisco-IP-Camera-2500	50	6
Valid	Built-in	Cisco-IP-Camera-2520	50	7
Valid	Built-in	Cisco-IP-Camera-2530	50	8
Valid	Built-in	Cisco-IP-Camera-4xxx	50	9
Valid	Built-in	Cisco-Transparent-Bridge	8	10
Valid	Built-in	Transparent-Bridge	8	11
Valid	Built-in	Cisco-Source-Bridge	10	12
Valid	Built-in	Cisco-Switch	10	13
Valid	Built-in	Cisco-IP-Phone	20	14
Valid	Built-in	IP-Phone	20	15
Valid	Built-in	Cisco-DMP	10	16
Valid	Built-in	Cisco-DMP-4305G	70	17
Valid	Built-in	Cisco-DMP-4310G	70	18
Valid	Built-in	Cisco-DMP-4400G	70	19
Valid	Built-in	Cisco-WLC-2100-Series	40	20
Valid	Built-in	Cisco-Access-Point	10	21
Valid	Built-in	Cisco-AIR-LAP	30	22
Valid	Built-in	Cisco-AIR-AP	30	23
Valid	Built-in	Linksys-Device	20	24

show environment

ファン、温度、および電源の情報を表示するには、EXEC モードで **show environment** コマンドを使用します。

show environment { **all** | **fan** | **power** | **stack** | **temperature** }

Syntax Description

all	ファンおよび温度の環境ステータスおよび内部電源装置のステータスを表示します。
fan	スイッチのファンの状態を表示します。
power	アクティブスイッチの内部電源の状態を表示します。
stack	スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。 このキーワードは、スタック構成対応スイッチでだけ使用できません。
temperature	スイッチの温度ステータスを表示します。

Command Default

なし

Command Modes

ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

アクセスされているスイッチ（スタンドアロンスイッチまたはアクティブスイッチ）の情報を表示するには、**show environment EXEC** コマンドを使用します。スタックまたは指定されたスタックメンバーのすべての情報を表示するには、**stack** キーワードを指定してこのコマンドを使用します。

show environment temperature status コマンドを入力すると、コマンド出力にスイッチの温度状態としきい値レベルが表示されます。

show environment temperature コマンドを使用して、スイッチの温度状態を表示することもできます。コマンド出力では、GREEN および YELLOW ステートを **OK** と表示し、RED ステートを **FAULTY** と表示します。

Examples

この例は、**show environment all** コマンドのサンプル出力を示しています：

```
Device> show environment all

Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
Inlet Temperature Value: 25 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold    : 56 Degree Celsius

Hotspot Temperature Value: 35 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold    : 125 Degree Celsius
SW  PID                Serial#      Status      Sys Pwr  PoE Pwr  Watts
---  -
1A  Unknown              Unknown     No Input Power Bad      Bad      235
1B  PWR-C1-350WAC        DCB2137H04P OK          Good     Good     350
```

この例は、**show environment power** コマンドのサンプル出力を示しています:

```
Device> show environment power

SW  PID                Serial#      Status      Sys Pwr  PoE Pwr  Watts
---  -
1A  Unknown              Unknown     No Input Power Bad      Bad      235
1B  PWR-C1-350WAC        DCB2137H04P OK          Good     Good     350
```

この例は、**show environment stack** コマンドのサンプル出力を示しています:

```
Device# show environment stack

System Temperature Value: 41 Degree Celsius
System Temperature State: GREEN
Yellow Threshold : 66 Degree Celsius
Red Threshold    : 76 Degree Celsius
```

この例は、**show environment temperature** コマンドのサンプル出力を示しています:

```
Device> show environment temperature

Switch 1: SYSTEM TEMPERATURE is OK
Inlet Temperature Value: 25 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold    : 56 Degree Celsius

Hotspot Temperature Value: 35 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold    : 125 Degree Celsius
```

Table 15: show environment temperature status コマンド出力のステータス

状態	説明
緑	スイッチの温度が正常な動作範囲にあります。
イエロー	温度が警告範囲にあります。スイッチの外の周辺温度を確認する必要があります。

状態	説明
レッド	温度がクリティカル範囲にあります。温度がこの範囲にある場合、スイッチが正常に実行されない可能性があります。

show errdisable detect

errdisable 検出ステータスを表示するには、EXEC モードで **show errdisable detect** コマンドを使用します。

show errdisable detect

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes ユーザ EXEC (>)

特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines gbic-invalid エラーの理由は、無効な Small Form-Factor Pluggable (SFP) モジュールを意味します。コマンド出力内の **errdisable** の理由がアルファベット順に表示されます。Mode 列は、errdisable が機能ごとにどのように設定されているかを示します。

errdisable 検出は次のモードで設定できます。

- ポート モード: 違反が発生した場合、物理ポート全体が errdisable になります。
- VLAN モード: 違反が発生した場合、VLAN が errdisable になります。
- ポート/VLAN モード: 一部のポートでは物理ポート全体が errdisable になり、その他のポートでは VLAN ごとに errdisable になります。

次に、**show errdisable detect** コマンドの出力例を示します。

```
Device> show errdisable detect
ErrDisable Reason    Detection    Mode
-----
arp-inspection       Enabled     port
bpduguard            Enabled     vlan
channel-misconfig    Enabled     port
community-limit      Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap              Enabled     port
gbic-invalid          Enabled     port
inline-power          Enabled     port
invalid-policy        Enabled     port
l2ptguard             Enabled     port
link-flap             Enabled     port
loopback              Enabled     port
```

show errdisable detect

```
lsgroup          Enabled    port
pagp-flap        Enabled    port
psecure-violatio Enabled    port/vlan
security-violatio Enabled    port
sfp-config-mismat Enabled    port
storm-control    Enabled    port
udld              Enabled    port
vmps              Enabled    port
```

show errdisable recovery

errdisable 回復タイマー情報を表示するには、EXEC モードで **show errdisable recovery** コマンドを使用します。

show errdisable recovery

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines gbic-invalid error-disable の理由は、無効な Small Form-Factor Pluggable (SFP) インターフェイスを意味します。



Note unicast-flood フィールドは、出力に表示はされませんが無効です。

show ip interface

IP に設定されているインターフェイスのユーザビリティステータスを表示するには、特権 EXEC モードで **show ip interface** コマンドを使用します。

show ip interface [*type number*] [**brief**]

Syntax Description	<i>type</i> (任意) インターフェイスタイプ。
	<i>number</i> (任意) インターフェイス番号。
	brief (任意) 各インターフェイスのユーザビリティステータスの概要を表示します。
	Note show ip interface brief コマンドの出力には、対応するネットワークモジュールが接続されているかどうかに関係なく、使用可能なすべてのインターフェイスの情報が表示されます。それらのインターフェイスのうち、ネットワークモジュールが接続されているインターフェイスは設定が可能です。接続されているネットワークモジュールを確認するには、 show interface status コマンドを実行します。

Command Default IP に設定されているすべてのインターフェイスの完全なユーザビリティステータスが表示されます。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines インターフェイスが使用可能な場合（つまりパケットの送受信が可能な場合）、Cisco IOS ソフトウェアは、直接接続されているルートをルーティングテーブルに自動的に入力します。インターフェイスが使用可能でない場合は、直接接続されているルーティングエントリがルーティングテーブルから削除されます。エントリを削除することにより、ソフトウェアはダイナミックルーティングプロトコルを使用してネットワークへのバックアップルートを決定できません（存在する場合）。

インターフェイスが双方向通信を提供できる場合、回線プロトコルは「up」とマークされます。インターフェイスのハードウェアが使用できる場合、インターフェイスはupとマークされます。

オプションでインターフェイスタイプを指定すると、その特定のインターフェイスに関する情報が表示されます。省略可能な引数を指定しない場合は、すべてのインターフェイスに関する情報が表示されます。

PPP またはシリアル ライン インターネット プロトコル (SLIP) によって非同期インターフェイスがカプセル化されると、IP 高速スイッチングがイネーブルになります。 **show ip interface** コマン

ドを PPP または SLIP でカプセル化された非同期インターフェイスで実行すると、IP ファストスイッチングがイネーブルであることを示すメッセージが表示されます。

show ip interface brief コマンドを使用すると、デバイスインターフェイスのサマリーを表示できます。このコマンドでは、IP アドレス、インターフェイスのステータス、およびその他の情報が表示されます。

show ip interface brief コマンドでは、ユニキャスト RPF に関連する情報は表示されません。

Examples

次に、ギガビットイーサネットインターフェイス 1/0/1 のインターフェイス情報の例を示します。

```
Device# show ip interface gigabitethernet 1/0/1

GigabitEthernet1/0/1 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
  IP Input features, "PBR",
    are not supported by MPF and are IGNORED
  IP Output features, "NetFlow",
    are not supported by MPF and are IGNORED
```

次に、特定の VLAN のユーザビリティステータスを表示する例を示します。

```
Device# show ip interface vlan 1

Vlan1 is up, line protocol is up
```

show ip interface

```

Internet address is 10.0.0.4/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Sampled Netflow is disabled
IP multicast multilayer switching is disabled
Netflow Data Export (hardware) is enabled
    
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 16: show ip interface のフィールドの説明

フィールド	説明
Broadcast address is	ブロードキャストアドレス。
Peer address is	ピアアドレス。
MTU is	インターフェイスに設定されている MTU 値 (バイト)。
Helper address	ヘルパーアドレス (設定されている場合)。
Directed broadcast forwarding	ダイレクトブロードキャスト転送がイネーブルであるかどうかを示します。
Outgoing access list	インターフェイスに発信アクセスリストが設定されているかどうかを示します。

フィールド	説明
Inbound access list	インターフェイスに着信アクセスリストが設定されているかどうかを示します。
Proxy ARP	インターフェイスに対してプロキシ Address Resolution Protocol (ARP) がイネーブルであるかどうかを示します。
Security level	このインターフェイスに対して設定されている IP Security Option (IPSO) セキュリティ レベル。
Split horizon	スプリットホライズンがイネーブルであるかどうかを示します。
ICMP redirects	このインターフェイスでリダイレクトメッセージが送信されるかどうかを示します。
ICMP unreachable	このインターフェイスで到達不能メッセージが送信されるかどうかを示します。
ICMP mask replies	このインターフェイスでマスク応答が送信されるかどうかを示します。
IP fast switching	このインターフェイスに対してファストスイッチングがイネーブルであるかどうかを示します。通常、このようなシリアルインターフェイスではイネーブルになります。
IP Flow switching	このインターフェイスに対してフロースイッチングがイネーブルであるかどうかを示します。
IP CEF switching	インターフェイスに対して Cisco Express Forwarding スwitching がイネーブルであるかどうかを示します。
IP multicast fast switching	インターフェイスに対してマルチキャスト ファスト スwitching がイネーブルであるかどうかを示します。
IP route-cache flags are Fast	インターフェイスで NetFlow がイネーブルであるかどうかを示します。インターフェイスで NetFlow がイネーブルになっている場合は、「Flow init」と表示されます。 ip flow ingress コマンドを使用してサブインターフェイスで NetFlow がイネーブルになっている場合は、「Ingress Flow」と表示されます。 ip route-cache flow コマンドを使用してメインインターフェイスで NetFlow がイネーブルになっている場合は、「Flow」と表示されます。
Router Discovery	このインターフェイスに対して探索プロセスがイネーブルであるかどうかを示します。通常、シリアルインターフェイスではディセーブルになります。
IP output packet accounting	このインターフェイスに対して IP アカウンティングがイネーブルであるかどうかとしいき値（エントリの最大数）を示します。

show ip interface

フィールド	説明
TCP/IP header compression	圧縮がイネーブルであるかどうかを示します。
WCCP Redirect outbound is disabled	インターフェイスで受信されたパケットがキャッシュエンジンにリダイレクトされるかどうかのステータスを示します。「enabled」または「disabled」のいずれかが表示されます。
WCCP Redirect exclude is disabled	インターフェイスへ向かうパケットがキャッシュエンジンへのリダイレクトから除外されるかどうかのステータスを示します。「enabled」または「disabled」のいずれかが表示されます。
Netflow Data Export (hardware) is enabled	インターフェイスの NetFlow データエクスポート (NDE) ハードウェア フロー ステータス。

次に、各インターフェイスのユーザビリティステータス情報のサマリーを表示する例を示します。

Device# **show ip interface brief**

```

Interface          IP-Address      OK? Method Status          Protocol
Vlan1              unassigned     YES NVRAM   administratively down  down
GigabitEthernet0/0 unassigned     YES NVRAM   down            down
GigabitEthernet1/0/1 unassigned     YES NVRAM   down            down
GigabitEthernet1/0/2 unassigned     YES unset   down            down
GigabitEthernet1/0/3 unassigned     YES unset   down            down
GigabitEthernet1/0/4 unassigned     YES unset   down            down
GigabitEthernet1/0/5 unassigned     YES unset   down            down
GigabitEthernet1/0/6 unassigned     YES unset   down            down
GigabitEthernet1/0/7 unassigned     YES unset   down            down
    
```

<output truncated>

Table 17: show ip interface brief のフィールドの説明

フィールド	説明
Interface	インターフェイスのタイプ。
IP-Address	インターフェイスに割り当てられている IP アドレス。
OK?	「Yes」は、その IP アドレスが有効であることを意味します。「No」は、その IP アドレスが有効でないことを意味します。

フィールド	説明
Method	<p>Method フィールドの値は次のとおりです。</p> <ul style="list-style-type: none"> • RARP または SLARP: Reverse Address Resolution Protocol (RARP) または Serial Line Address Resolution Protocol (SLARP) 要求。 • BOOTP: ブートストラッププロトコル。 • TFTP: TFTP サーバから取得したコンフィギュレーションファイル。 • manual: コマンドラインインターフェイスでの手動変更。 • NVRAM: NVRAM のコンフィギュレーションファイル。 • IPCP: ip address negotiated コマンド。 • DHCP: ip address dhcp コマンド。 • unset: 未設定。 • other: 不明。
Status	<p>インターフェイスのステータスを示します。有効な値とその意味は次のとおりです。</p> <ul style="list-style-type: none"> • up: インターフェイスはアップ状態です。 • down: インターフェイスはダウン状態です。 • administratively down: インターフェイスは管理上の目的でダウンしています。
Protocol	このインターフェイス上のルーティングプロトコルの稼働ステータスを示します。

Related Commands

Command	Description
ip interface	Secure Socket Layer Virtual Private Network (SSL VPN) ゲートウェイの仮想ゲートウェイ IP インターフェイスを設定します。
show interface status	インターフェイスの状態が表示されます。

show interfaces

すべてのインターフェイスまたは指定したインターフェイスの管理ステータスおよび動作ステータスを表示するには、EXEC モードで **show interfaces** コマンドを使用します。

```
show interfaces [ interface-id | vlan vlan-id ] [ accounting | capabilities [ module number ]
| description | etherchannel | flowcontrol | link [ module number ] | private-vlan mapping | pruning
| stats | status [ err-disabled | inactive ] | trunk ]
```

Syntax Description

<i>interface-id</i>	<p>(任意) インターフェイスの ID です。有効なインターフェイスには、物理ポート (タイプ、スタック構成可能なスイッチのスタックメンバ、モジュール、およびポート番号を含む) やポート チャンネルが含まれます。</p> <p>指定できるポートチャンネルは 1 ~ 48 です。</p>
vlan <i>vlan-id</i>	<p>(任意) VLANID です。指定できる範囲は 1 ~ 4094 です。</p>
accounting	<p>(任意) インターフェイスのアカウント情報 (アクティブ プロトコル、入出力のパケット、オクテットを含む) を表示します。</p> <p>Note ソフトウェアで処理されたパケットだけが表示されます。ハードウェアでスイッチングされるパケットは表示されません。</p>
capabilities	<p>(任意) すべてのインターフェイスまたは指定されたインターフェイスの性能 (機能、インターフェイス上で設定可能なオプションを含む) を表示します。このオプションはコマンドラインのヘルプに表示されますが、VLANID に使用できません。</p>
module <i>number</i>	<p>(任意) スイッチまたは指定されたスタックメンバのすべてのインターフェイスの機能を表示します。</p> <p>このオプションは、特定のインターフェイス ID を入力したときは利用できません。</p>

description	<p>(任意) インターフェイスに設定された管理ステータスおよび説明を表示します。</p> <p>Note show interfaces description コマンドの出力には、対応するネットワークモジュールが接続されているかどうかに関係なく、使用可能なすべてのインターフェイスの情報が表示されます。それらのインターフェイスのうち、ネットワークモジュールが接続されているインターフェイスは設定が可能です。接続されているネットワークモジュールを確認するには、show interface status コマンドを実行します。</p>
etherchannel	(任意) インターフェイス EtherChannel 情報を表示します。
flowcontrol	(任意) インターフェイスのフロー制御情報を表示します。
link [modulenumbers]	(任意) インターフェイスのアップタイムとダウンタイムを表示します。
private-vlan mapping	(任意) VLAN スイッチ仮想インターフェイス (SVI) のプライベート VLAN のマッピング情報を表示します。スイッチが LAN Base フィーチャセットを実行している場合、このキーワードは使用できません。
pruning	(任意) インターフェイスのトランク VTP プルーニング情報を表示します。
stats	(任意) インターフェイスのパスを切り替えることによる入出力パケットを表示します。
status	(任意) インターフェイスのステータスを表示します。Type フィールドの unsupported のステータスは、他社製の Small Form-Factor Pluggable (SFP) モジュールがモジュール スロットに装着されていることを示しています。
err-disabled	(任意) errdisable ステートのインターフェイスを表示します。
inactive	(任意) 非アクティブステートのインターフェイスを表示します。
trunk	(任意) インターフェイス トランク情報を表示します。インターフェイスを指定しない場合は、アクティブな トラン キング ポートの情報だけが表示されます。



Note **crb**、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**random-detect**、**rate-limit**、および**shape** キーワードはコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

Command Default なし

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Gibraltar 16.12.1	link キーワードが導入されました。

Usage Guidelines **show interfaces capabilities** コマンドに異なるキーワードを指定することで、次のような結果になります。

- **show interface capabilities module number** コマンドを使用して、スタックのスイッチ上のすべてのインターフェイスの機能を表示します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。
- 指定されたインターフェイスの機能を表示するには、**show interfaces interface-id capabilities** を使用します。
- スタック内のすべてのインターフェイスの機能を表示するには、**show interfaces capabilities** を使用します（モジュール番号またはインターフェイス ID の指定なし）。



Note コマンド出力に表示される **Last Input** フィールドは、最後のパケットがインターフェイスによって正常に受信され、デバイスの CPU によって処理されてから経過した時間、分、および秒数を示します。この情報は、デッドインターフェイスに障害が発生した時間を知るために使用できます。

Last Input は、ファースト スwitチングされたトラフィックでは更新されません。

コマンド出力に表示される **output** フィールドは、最後のパケットがインターフェイスによって正常に送信されてから経過した時間、分、および秒数を示します。このフィールドによって示される情報は、デッドインターフェイスに障害が発生した時間を知るために役立ちます。

show interfaces link コマンドに異なるキーワードを指定することで、次のような結果が得られます。

- **show interface link module** *number* コマンドを使用して、スタック内のスイッチ上のすべてのインターフェイスのアップタイムとダウンタイムを表示します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。



Note スタンドアロンスイッチでは、**module number** はスロット番号を表します。

- 指定したインターフェイスのアップタイムとダウンタイムを表示するには、**show interfaces interface-id link** を使用します。
- スタック内のすべてのインターフェイスのアップタイムとダウンタイムを表示するには、**show interfaces link** を使用します（モジュール番号またはインターフェイス ID の指定なし）。
- インターフェイスがアップ状態の場合、アップタイムには時間（時、分、秒）が表示され、ダウンタイムには 00:00:00 が表示されます。
- インターフェイスがダウン状態の場合、ダウンタイムには時間（時、分、秒）が表示されません。

Examples

次の例では、スタック メンバ 3 のインターフェイスに対する **show interfaces** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet3/0/2

GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out
```

```

Device# show interfaces accounting

Vlan1
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
      IP          0         0           6          378
Vlan200
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/0
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
      Other      165476   11417844   0          0
      Spanning Tree 1240284  64494768   0          0
      ARP        7096    425760    0          0
      CDP        41368   18781072   82908     35318808
GigabitEthernet1/0/1
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

<output truncated>

```

次の例では、**description** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを *Connects to Marketing* として指定した場合の **show interfaces interface description** コマンドの出力を示します。

```

Device# show interfaces gigabitethernet1/0/2 description

Interface          Status          Protocol Description
Gi1/0/2            up              down          Connects to Marketing

```

```

Device# show interfaces etherchannel
----
Port-channel34:
Age of the Port-channel   = 28d:18h:51m:46s
Logical slot/port        = 12/34          Number of ports = 0
GC                       = 0x00000000      HotStandBy port = null
Passive port list        =
Port state                = Port-channel L3-Ag Ag-Not-Inuse
Protocol                  = -
Port security             = Disabled

```

次の例では、VTP ドメイン内でプルーンングがイネーブルの場合の **show interfaces interface-id pruning** コマンドの出力を示します。

```

Device# show interfaces gigabitethernet1/0/2 pruning

Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3

```

次の例では、指定した VLAN インターフェイスの **show interfaces stats** コマンドの出力を示します。

```

Device# show interfaces vlan 1 stats

Switching path   Pkts In   Chars In   Pkts Out   Chars Out

```

```

Processor      1165354  136205310  570800  91731594
Route cache    0         0          0        0
Total          1165354  136205310  570800  91731594
    
```

次に、**show interfaces status err-disabled** コマンドの出力例を示します。errdisable ステータスのインターフェイスのステータスを表示します。

```

Device# show interfaces status err-disabled

Port      Name      Status      Reason
Gi1/0/2   err-disabled  gbic-invalid
Gi2/0/3   err-disabled  dtp-flap
    
```

次の例では、**show interfaces interface-id pruning** コマンドの出力例を示します。

```

Device# show interfaces gigabitethernet1/0/2 pruning

Port Vlans pruned for lack of request by neighbor

Device# show interfaces gigabitethernet1/0/1 trunk

Port      Mode      Encapsulation  Status      Native vlan
Gi1/0/1   on        802.1q         other       10

Port      Vlans allowed on trunk
Gi1/0/1   none

Port      Vlans allowed and active in management domain
Gi1/0/1   none

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/1   none
    
```

次に、**show interfaces description** コマンドの出力例を示します。

```

Device# show interfaces description

Interface      Status      Protocol Description
Vl1            admin down  down
Gi0/0          down       down
Gi1/0/1        down       down
Gi1/0/2        down       down
Gi1/0/3        down       down
Gi1/0/4        down       down
Gi1/0/5        down       down
Gi1/0/6        down       down
Gi1/0/7        down       down

<output truncated>
    
```

次に、**show interfaces link** コマンドの出力例を示します。

```

Device> enable
Device# show interfaces link

Port      Name      Down Time      Up Time
Gi1/0/1   Gi1/0/1   6w0d
Gi1/0/2   Gi1/0/2   6w0d
Gi1/0/3   Gi1/0/3   00:00:00      5w3d
Gi1/0/4   Gi1/0/4   6w0d
    
```

show interfaces

```
Gi1/0/5          6w0d
Gi1/0/6          6w0d
Gi1/0/7          6w0d
Gi1/0/8          6w0d
Gi1/0/9          6w0d
Gi1/0/10         6w0d
Gi1/0/11        2d17h
Gi1/0/12         6w0d
Gi1/0/13         6w0d
Gi1/0/14         6w0d
Gi1/0/15         6w0d
Gi1/0/16         6w0d
Gi1/0/17         6w0d
Gi1/0/18         6w0d
Gi1/0/19         6w0d
Gi1/0/20         6w0d
Gi1/0/21         6w0d
```

show interfaces counters

スイッチまたは特定のインターフェイスのさまざまなカウンタを表示するには、特権 EXEC モードで **show interfaces counters** コマンドを使用します。

show interfaces [*interface-id*] **counters** [**errors** | **etherchannel** | **module** *member-number* | **protocol status** | **trunk**]

Syntax Description	
<i>interface-id</i>	(任意) 物理インターフェイスの ID (タイプ、スタックメンバ (スタック構成可能なスイッチのみ)、モジュール、ポート番号を含む)。
errors	(任意) エラー カウンタを表示します。
etherchannel	(任意) 送受信されたオクテット、ブロードキャストパケット、マルチキャストパケット、およびユニキャストパケットなど、EtherChannel カウンタを表示します。
module <i>member-number</i>	(任意) 指定されたメンバのカウンタを表示します。 指定できる範囲は 1 ~ 9 です。 Note このコマンドでは、 module キーワードはスタックメンバ番号を参照しています。インターフェイス ID に含まれるモジュール番号は、常に 0 です。
protocol status	(任意) インターフェイスでイネーブルになっているプロトコルのステータスを表示します。
trunk	(任意) トランク カウンタを表示します。



Note **vlan** *vlan-id* キーワードは、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。

Command Default	なし	
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines キーワードを入力しない場合は、すべてのインターフェイスのすべてのカウンタが表示されます。

次の例では、**show interfaces counters** コマンドの出力の一部を示します。スイッチのすべてのカウンタが表示されます。

```
Device# show interfaces counters
Port          InOctets      InUcastPkts   InMcastPkts   InBcastPkts
Gi1/0/1       0              0              0              0
Gi1/0/2       0              0              0              0
Gi1/0/3       95285341      43115         1178430       1950
Gi1/0/4       0              0              0              0
```

<output truncated>

次の例では、モジュール 2 に対する **show interfaces counters module** コマンドの出力の一部を示します。モジュール内の指定したスイッチのすべてのカウンタが表示されます。

```
Device# show interfaces counters module 2
Port          InOctets      InUcastPkts   InMcastPkts   InBcastPkts
Gi1/0/1       520           2              0              0
Gi1/0/2       520           2              0              0
Gi1/0/3       520           2              0              0
Gi1/0/4       520           2              0              0
```

<output truncated>

次の例では、すべてのインターフェイスに対する **show interfaces counters protocol status** コマンドの出力の一部を示します。

```
Device# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP
```

<output truncated>

次に、**show interfaces counters trunk** コマンドの出力例を示します。すべてのインターフェイスのトランク カウンタが表示されます。

```
Device# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/0/1       0              0              0
```

```
Gi1/0/2          0          0          0
Gi1/0/3          80678       0          0
Gi1/0/4          82320       0          0
Gi1/0/5          0           0          0
```

```
<output truncated>
```

show interfaces switchport

ポートブロッキング、ポート保護設定など、スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示するには、特権 EXEC モードで **show interfaces switchport** コマンドを使用します。

show interfaces [*interface-id*] **switchport** [*module number*]

Syntax Description	<p><i>interface-id</i> (任意) インターフェイスの ID です。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタックメンバ、モジュール、およびポート番号を含む）やポート チャンルが含まれます。指定できるポートチャンネルは 1 ~ 48 です。</p> <hr/> <p>module number (任意) スイッチまたは指定されたスタックメンバのすべてのインターフェイスのスイッチポート設定を表示します。</p> <p>このオプションは、特定のインターフェイス ID を入力したときは利用できません。</p>				
Command Default	なし				
Command Modes	特権 EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines スタックのスイッチ上のすべてのインターフェイスのスイッチポート特性を表示するには、**show interface switchport module number** コマンドを使用します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。

次の例では、ポートの **show interfaces switchport** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
```

```

Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
    
```

フィールド	説明
Name	ポート名を表示します。
Switchport	ポートの管理ステータスおよび動作ステータスを表示します。この出力の場合、ポートはスイッチポートモードです。
Administrative Mode Operational Mode	管理モードおよび動作モードを表示します。
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	管理上および運用上のカプセル化方式、およびトランキングネゴシエーションがイネーブルかどうかを表示します。
Access Mode VLAN	ポートを設定する VLAN ID を表示します。
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	ネイティブモードのトランクの VLAN ID を一覧表示します。トランク上の許可 VLAN を一覧表示します。トランク上のアクティブ VLAN を一覧表示します。
Pruning VLANs Enabled	プルーニングに適格な VLAN を一覧表示します。
Protected	インターフェイス上で保護ポートがイネーブル (True) であるかまたはディセーブル (False) であるかを表示します。
Unknown unicast blocked Unknown multicast blocked	不明なマルチキャストおよび不明なユニキャストトラフィックがインターフェイス上でブロックされているかどうかを表示します。
Voice VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。

show interfaces switchport

フィールド	説明
Appliance trust	IP Phone のデータ パケットのサービス クラス (CoS) 設定を表示します。

show interfaces transceiver

Small Form-Factor Pluggable (SFP) モジュールインターフェイスの物理インターフェイスを表示するには、EXEC モードで **show interfaces transceiver** コマンドを使用します。

show interfaces [*interface-id*] **transceiver** [**detail** | **module** *number* | **properties** | **supported-list** | **threshold-table**]

Syntax Description	
<i>interface-id</i>	(任意) 物理インターフェイスのID (タイプ、スタックメンバ (スタック構成可能なスイッチのみ)、モジュール、ポート番号を含む)。
detail	(任意) (スイッチにインストールされている場合) Digital Optical Monitoring (DoM) 対応トランシーバの高低値やアラーム情報などの、調整プロパティを表示します。
module <i>number</i>	(任意) スwitchのモジュールのインターフェイスへの表示を制限します。 このオプションは、特定のインターフェイスIDを入力したときは利用できません。
properties	(任意) インターフェイスの速度、デュプレックス、およびインラインパワー設定を表示します。
supported-list	(任意) サポートされるトランシーバをすべて表示します。
threshold-table	(任意) アラームおよび警告しきい値テーブルを表示します。

Command Modes	
	ユーザ EXEC (>)
	特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の例では、**show interfaces interface-id transceiver properties** コマンドの出力を示します。

```
Device# show interfaces transceiver
```

```
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
```

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
Gi5/1/2	42.9	3.28	22.1	-5.4	-8.1

show interfaces transceiver

```
Te5/1/3      32.0      3.28      19.8      2.4      -4.2
```

Device# **show interfaces gigabitethernet1/1/1 transceiver properties**

```
Name : Gi1/1/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

次の例では、**show interfaces interface-id transceiver detail** コマンドの出力を示します。

Device# **show interfaces gigabitethernet1/1/1 transceiver detail**

```
ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1/1	29.9	74.0	70.0	0.0	-4.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1/1	3.28	3.60	3.50	3.10	3.00

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	1.8	7.9	3.9	0.0	-4.0

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	-23.5	-5.0	-9.0	-28.2	-32.2

Device# **show interfaces transceiver supported-list**

```
Transceiver Type      Cisco p/n min version
                        supporting DOM
-----
DWDM GBIC             ALL
DWDM SFP              ALL
RX only WDM GBIC     ALL
DWDM XENPAK          ALL
DWDM X2               ALL
DWDM XFP              ALL
CWDM GBIC             NONE
CWDM X2               ALL
CWDM XFP              ALL
XENPAK ZR             ALL
```

```

X2 ZR                ALL
XFP ZR                ALL
Rx_only_WDM_XENPAK  ALL
XENPAK_ER            10-1888-04
X2_ER                ALL
XFP_ER                ALL
XENPAK_LR            10-1838-04
X2_LR                ALL
XFP_LR                ALL
XENPAK_LW            ALL
X2_LW                ALL
XFP_LW                NONE
XENPAK_SR            NONE
X2_SR                ALL
XFP_SR                ALL
XENPAK_LX4           NONE
X2_LX4               NONE
XFP_LX4              NONE
XENPAK_CX4           NONE
X2_CX4               NONE
XFP_CX4              NONE
SX_GBIC              NONE
LX_GBIC              NONE
ZX_GBIC              NONE
CWDM_SFP             ALL
Rx_only_WDM_SFP     NONE
SX_SFP               ALL
LX_SFP               ALL
ZX_SFP               ALL
EX_SFP               ALL
SX_SFP               NONE
LX_SFP               NONE
ZX_SFP               NONE
GigE_BX_U_SFP       NONE
GigE_BX_D_SFP       ALL
X2_LRM               ALL
SR_SFPP              ALL
LR_SFPP              ALL
LRM_SFPP             ALL
ER_SFPP              ALL
ZR_SFPP              ALL
DWDM_SFPP            ALL
GigE_BX_40U_SFP     ALL
GigE_BX_40D_SFP     ALL
GigE_BX_40DA_SFP    ALL
GigE_BX_80U_SFP     ALL
GigE_BX_80D_SFP     ALL
GIG_BXU_SFPP        ALL
GIG_BXD_SFPP        ALL
GIG_BX40U_SFPP      ALL
GIG_BX40D_SFPP      ALL
GigE_Dual_Rate_LX_SFP ALL
CWDM_SFPP            ALL
CPAK_SR10            ALL
CPAK_LR4             ALL
QSFP_LR              ALL
QSFP_SR              ALL
    
```

次に、**show interfaces transceiver threshold-table** コマンドの出力例を示します。

```

Device# show interfaces transceiver threshold-table
          Optical Tx      Optical Rx      Temp      Laser Bias      Voltage
                   current
    
```

show interfaces transceiver

```

-----
      DWDM GBIC
Min1      -4.00      -32.00      -4          N/A          4.65
Min2      0.00      -28.00      0           N/A          4.75
Max2      4.00      -9.00      70          N/A          5.25
Max1      7.00      -5.00      74          N/A          5.40
      DWDM SFP
Min1      -4.00      -32.00      -4          N/A          3.00
Min2      0.00      -28.00      0           N/A          3.10
Max2      4.00      -9.00      70          N/A          3.50
Max1      8.00      -5.00      74          N/A          3.60
      RX only WDM GBIC
Min1      N/A        -32.00      -4          N/A          4.65
Min2      N/A        -28.30      0           N/A          4.75
Max2      N/A        -9.00      70          N/A          5.25
Max1      N/A        -5.00      74          N/A          5.40
      DWDM XENPAK
Min1      -5.00      -28.00      -4          N/A          N/A
Min2      -1.00      -24.00      0           N/A          N/A
Max2      3.00      -7.00      70          N/A          N/A
Max1      7.00      -3.00      74          N/A          N/A
      DWDM X2
Min1      -5.00      -28.00      -4          N/A          N/A
Min2      -1.00      -24.00      0           N/A          N/A
Max2      3.00      -7.00      70          N/A          N/A
Max1      7.00      -3.00      74          N/A          N/A
      DWDM XFP
Min1      -5.00      -28.00      -4          N/A          N/A
Min2      -1.00      -24.00      0           N/A          N/A
Max2      3.00      -7.00      70          N/A          N/A
Max1      7.00      -3.00      74          N/A          N/A
      CWDM X2
Min1      N/A        N/A        0           N/A          N/A
Min2      N/A        N/A        0           N/A          N/A
Max2      N/A        N/A        0           N/A          N/A
Max1      N/A        N/A        0           N/A          N/A

```

<output truncated>

Related Commands

コマンド	説明
transceiver type all	トランシーバ タイプ コンフィギュレーション モードを
monitoring	デジタル オプティカル モニタリングを有効にします。

show macro auto

Auto SmartPort マクロの情報を表示するには、ユーザ EXEC モードで **show macro auto** コマンドを使用します。

```
show macro auto {address-group address-group-name | device [access-point] [ip-camera]
[lightweight-ap] [media-player] [phone] [router] [switch] | global [event_trigger] | interface
[interface_id]}
```

Syntax Description

address-group [<i>address-group-name</i>]	アドレスグループ情報を表示します。 (任意) <i>address-group-name</i> : 指定したアドレスグループの情報を表示します。
device [<i>access-point</i>] [<i>ip-camera</i>] [<i>lightweight-ap</i>] [<i>media-player</i>] [<i>phone</i>] [<i>router</i>] [<i>switch</i>]	1つ以上のデバイスの情報を表示します。 <ul style="list-style-type: none"> • (任意) access-point: Autonomous アクセスポイント • (任意) ip-camera: Cisco IP ビデオ監視カメラ • (任意) lightweight-ap: 中央管理型 アクセスポイント • (任意) media-player: デジタルメディアプレーヤー • (任意) phone: Cisco IP 電話 • (任意) router: Cisco ルータ • (任意) switch: Cisco スイッチ
global [<i>event_trigger</i>]	スイッチの Auto Smartport 情報を表示します。 (任意) <i>event_trigger</i> : 指定したイベントトリガーの情報を表示します。
interface [<i>interface_id</i>]	インターフェイスのステータスを表示します。 (任意) <i>interface_id</i> : 指定したインターフェイスの情報を表示します。

Command Modes

ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スイッチの Auto SmartPort 情報を表示するには、このコマンドを使用します。デバイスの設定可能なパラメータを表示するには、**show macro auto device** コマンドを使用します。

例

次に、**show macro auto device** を使用してスイッチの設定を表示する例を示します。

```

Device# show macro auto device
Device:lightweight-ap
Default Macro:CISCO_LWAP_AUTO_SMARTPORT
Current Macro:CISCO_LWAP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=1

Device:access-point
Default Macro:CISCO_AP_AUTO_SMARTPORT
Current Macro:CISCO_AP_AUTO_SMARTPORT
Configurable Parameters:NATIVE_VLAN
Defaults Parameters:NATIVE_VLAN=1
Current Parameters:NATIVE_VLAN=1

Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:ACCESS_VLAN=1 VOICE_VLAN=2

Device:router
Default Macro:CISCO_ROUTER_AUTO_SMARTPORT
Current Macro:CISCO_ROUTER_AUTO_SMARTPORT
Configurable Parameters:NATIVE_VLAN
Defaults Parameters:NATIVE_VLAN=1
Current Parameters:NATIVE_VLAN=1

Device:switch
Default Macro:CISCO_SWITCH_AUTO_SMARTPORT
Current Macro:CISCO_SWITCH_AUTO_SMARTPORT
Configurable Parameters:NATIVE_VLAN
Defaults Parameters:NATIVE_VLAN=1
Current Parameters:NATIVE_VLAN=1

Device:ip-camera
Default Macro:CISCO_IP_CAMERA_AUTO_SMARTPORT
Current Macro:CISCO_IP_CAMERA_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=1

Device:media-player
Default Macro:CISCO_DMP_AUTO_SMARTPORT
Current Macro:CISCO_DMP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
    
```

```
Defaults Parameters:ACCESS_VLAN=1  
Current Parameters:ACCESS_VLAN=1
```

次に、**show macro auto address-group name** コマンドを使用してスイッチの TEST3 アドレスグループ設定を表示する例を示します。

```
Device# show macro auto address-group TEST3MAC Address Group Configuration:  
  
Group Name OUI   MAC ADDRESS  
-----  
TEST3 2233.33      0022.0022.0022  
2233.34
```

show memory platform

プラットフォームのメモリ統計情報を表示するには、特権 EXEC モードで **show memory platform** コマンドを使用します。

show memory platform [**compressed-swap** | **information** | **page-merging**]

Syntax Description	compressed-swap (任意) プラットフォーム メモリの圧縮スワップ情報を表示します。
	information (任意) プラットフォームに関する一般的な情報を表示します。
	page-merging (任意) プラットフォームメモリのページマージング情報を表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 空きメモリは正確に計算されて、コマンド出力の Free Memory フィールドに表示されます。

Examples

次に、**show memory platform** コマンドの出力例を示します。

```
Switch# show memory platform

Virtual memory   : 12874653696
Pages resident   : 627041
Major page faults: 2220
Minor page faults: 2348631

Architecture     : mips64
Memory (kB)
  Physical       : 3976852
  Total          : 3976852
  Used           : 2761276
  Free           : 1215576
  Active         : 2128196
  Inactive       : 1581856
  Inact-dirty    : 0
  Inact-clean    : 0
  Dirty          : 0
  AnonPages      : 1294984
  Bounce         : 0
  Cached         : 1978168
  Commit Limit   : 1988424
  Committed As   : 3343324
  High Total     : 0
  High Free      : 0
  Low Total      : 3976852
  Low Free       : 1215576
  Mapped         : 516316
  NFS Unstable   : 0
  Page Tables    : 17124
```

```

Slab          : 0
VMmalloc Chunk : 1069542588
VMmalloc Total : 1069547512
VMmalloc Used  : 2588
Writeback     : 0
HugePages Total: 0
HugePages Free : 0
HugePages Rsvd : 0
HugePage Size : 2048

Swap (kB)
Total        : 0
Used         : 0
Free         : 0
Cached       : 0

Buffers (kB) : 437136

Load Average
1-Min       : 1.04
5-Min       : 1.16
15-Min      : 0.94

```

次に、**show memory platform information** コマンドの出力例を示します。

```
Device# show memory platform information
```

```

Virtual memory : 12870438912
Pages resident : 626833
Major page faults: 2222
Minor page faults: 2362455

Architecture : mips64
Memory (kB)
Physical      : 3976852
Total        : 3976852
Used         : 2761224
Free         : 1215628
Active       : 2128060
Inactive     : 1584444
Inact-dirty  : 0
Inact-clean  : 0
Dirty        : 284
AnonPages    : 1294656
Bounce       : 0
Cached       : 1979644
Commit Limit : 1988424
Committed As : 3342184
High Total   : 0
High Free    : 0
Low Total    : 3976852
Low Free     : 1215628
Mapped       : 516212
NFS Unstable : 0
Page Tables  : 17096
Slab         : 0
VMmalloc Chunk : 1069542588
VMmalloc Total : 1069547512
VMmalloc Used  : 2588
Writeback     : 0
HugePages Total: 0
HugePages Free : 0

```

show memory platform

```
HugePages Rsvd : 0
HugePage Size : 2048

Swap (kB)
  Total      : 0
  Used       : 0
  Free       : 0
  Cached     : 0

Buffers (kB) : 438228

Load Average
  1-Min      : 1.54
  5-Min      : 1.27
  15-Min     : 0.99
```

show module

スイッチ番号、モデル番号、シリアル番号、ハードウェア リビジョン番号、ソフトウェアバージョン、MAC アドレスなどのモジュール情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで、このコマンドを使用します。

```
show module [switch-num]
```

Syntax Description	<i>switch-num</i>	(任意) スイッチの番号。
Command Default	なし	
Command Modes	ユーザ EXEC (>) 特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	<i>switch-num</i> 引数を指定せずに show module コマンドを入力した場合、 show module all コマンドを入力した場合と同じ結果になります。	

show network-policy profile

ネットワークポリシー プロファイルを表示するには、特権 EXEC モードで **show network policy profile** コマンドを使用します。

show network-policy profile [*profile-number*] [**detail**]

Syntax Description	<i>profile-number</i> (任意) ネットワークポリシー プロファイル番号を表示します。プロファイルが入力されていない場合、すべてのネットワーク ポリシープロファイルが表示されます。	
	detail	(任意) 詳細なステータスと統計情報を表示します。
Command Default	なし	
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show network-policy profile** コマンドの出力例を示します。

```
Device# show network-policy profile
Network Policy Profile 10
  voice vlan 17 cos 4
  Interface:
    none
Network Policy Profile 30
  voice vlan 30 cos 5
  Interface:
    none
Network Policy Profile 36
  voice vlan 4 cos 3
  Interface:
    Interface_id
```

show parser macro

スイッチ上で設定されているすべてのマクロ、または1つのマクロのパラメータを表示するには、ユーザ EXEC モードで **show parser macro** コマンドを使用します。

show parser macro {**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}

Syntax Description	brief	(任意) 各マクロの名前を表示します。
	description [interface <i>interface-id</i>]	(任意) すべてのマクロの説明または特定のインターフェイスの説明を表示します。
	name <i>macro-name</i>	(任意) マクロ名で特定された1つのマクロに関する情報を表示します。
Command Modes	ユーザ EXEC (>) 特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次の例では、**show parser macro** コマンドの出力の一部を示します。シスコデフォルトマクロの出力は、スイッチのプラットフォームとスイッチ上で実行しているソフトウェアイメージによって異なります。

```
Device# show parser macro
Total number of macros = 6
-----
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
errdisable recovery cause link-flap
errdisable recovery interval 60

<output truncated>

-----
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
```

<output truncated>

```
-----
Macro name : cisco-phone
Macro type : default interface
# Cisco IP phone + desktop template
# macro keywords $AVID $VVID
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
```

<output truncated>

```
-----
Macro name : cisco-switch
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Do not apply to EtherChannel/Port Group
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID
```

<output truncated>

```
-----
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID
```

<output truncated>

```
-----
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE
-----
```

次に、**show parser macro name** コマンドの出力例を示します。

```
Device# show parser macro name standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
```

```
channel-protocol pagp
```

次に、**show parser macro brief** コマンドの出力例を示します。

```
Device# show parser macro brief
default global      : cisco-global
default interface: cisco-desktop
default interface: cisco-phone
default interface: cisco-switch
default interface: cisco-router
customizable       : snmp
```

次に、**show parser macro description** コマンドの出力例を示します。

```
Device# show parser macro description
Global Macro(s): cisco-global
Interface      Macro Description(s)
-----
Gil/0/1        standard-switch10
Gil/0/2        this is test macro
-----
```

次に、**show parser macro description interface** コマンドの出力例を示します。

```
Device# show parser macro description interface gigabitethernet1/0/2
Interface      Macro Description
-----
Gil/0/2        this is test macro
-----
```

show platform hardware bluetooth

Bluetooth インターフェイスに関する情報を表示するには、特権 EXEC モードで **show platform hardware bluetooth** コマンドを使用します。

show platform hardware bluetooth

Command Default	なし	
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Usage Guidelines	show platform hardware bluetooth コマンドは、外部 USB Bluetooth ドングルがデバイスに接続されている場合に使用します。	

Examples

次に、**show platform hardware bluetooth** コマンドを使用して Bluetooth インターフェイスの情報を表示する例を示します。

```
Device> enable
Device# show platform hardware bluetooth
Controller: 0:1a:7d:da:71:13
Type: Primary
Bus: USB
State: DOWN
Name:
HCI Version:
```

show platform hardware fed switch forward interface

転送情報をデバッグし、ハードウェアのフォワーディングプレーンのパケットパスをトレースするには、**show platform hardware fed switch *switch_number* forward interface** コマンドを使用します。このコマンドは、ユーザ定義のパケットをシミュレートし、ハードウェアのフォワーディングプレーンから転送情報を取得します。このコマンドで指定したパケットパラメータに基づいて、入力ポートでパケットが生成されます。PCAP ファイルに格納されているキャプチャされたパケットから完全なパケットを提供することもできます。

このトピックでは、インターフェイス転送特有のオプション、つまり **show platform hardware fed switch {*switch_num* | active | standby } forward interface** コマンドで使用可能なオプションのみについて詳しく説明します。

```
show platform hardware fed switch {switch_num | active | standby} forward interface interface-type
interface-number source-mac-address destination-mac-address {protocol-number | arp | cos | ipv4 | ipv6
| mpls}
```

```
show platform hardware fed switch {switch_num | active | standby} forward interface interface-type
interface-number pcap pcap-file-name number packet-number data
```

```
show platform hardware fed switch {switch_num | active | standby} forward interface interface-type
interface-number vlan vlan-id source-mac-address destination-mac-address {protocol-number | arp |
cos | ipv4 | ipv6 | mpls}
```

Syntax Description

switch { <i>switch_num</i> active standby }	パケットのトレースをスケジュールするスイッチ。このスイッチで入力ポートが使用可能である必要があります。次のオプションがあります。 <ul style="list-style-type: none"> • switch_num: 入力ポートが存在するスイッチの ID。 • active: 入力ポートが存在するアクティブスイッチを示します。 • standby: 入力ポートが存在するスタンバイスイッチを示します。 <p>Note このキーワードはサポートされていません。</p>
interface <i>interface-type</i> <i>interface-number</i>	パケットのトレースをシミュレートする入力インターフェイス。
<i>source-mac-address</i>	シミュレートするパケットの送信元 MAC アドレス。
<i>destination-mac-address</i>	宛先インターフェイスの 16 進形式の MAC アドレス。
<i>protocol-number</i>	いずれかの L3 プロトコルに割り当てられた番号。
arp	Address Resolution Protocol (ARP) のパラメータ。
ipv4	IPv4 パケットのパラメータ。

show platform hardware fed switch forward interface

ipv6	IPv6 パケットのパラメータ。
mpls	マルチプロトコルラベルスイッチング (MPLS) ラベルのパラメータ。
cos	プライオリティを設定する 0 ~ 7 のサービスクラス (CoS) 値。
pcap <i>pcap-file-name</i>	内部フラッシュ (flash:) にある PCAP ファイルの名前。 ファイルが flash: にすでに存在していることを確認してください。
number <i>packet-number</i>	PCAP ファイル内のパケット番号を指定します。
vlan <i>vlan-id</i>	シミュレートされるパケットの dot1q ヘッダーの VLAN ID。指定できる範囲は 1 ~ 4096 です。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Fuji 16.9.1	このコマンドが拡張され、MPLS/ARP/VxLAN パケットのパラメータと PCAP ファイルでキャプチャされたパケットのトレースがサポートされるようになりました。
Cisco IOS XE Gibraltar 16.10.1	このコマンドが拡張され、スタック全体のデータのキャプチャがサポートされるようになりました。

Usage Guidelines

テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。

このコマンドでサポートされるパケットタイプは次のとおりです。

- いずれかの L3 プロトコルを使用する非 IP パケット
- ARP パケット
- いずれかの L4 プロトコルを使用する IPv4 パケット
- TCP/UDP/IGMP/ICMP/SCTP ペイロードで構成される IPv4 パケット
- VxLAN パケット

- 最大 3 つのラベルとメタデータで構成される MPLS パケット
- IPv4/IPv6 ペイロードで構成される MPLS パケット
- TCP/UDP/IGMP/ICMP/SCTP ペイロードで構成される IPv6 パケット

スタック環境では、スタックメンバの数やトポロジに関係なく、スタック全体の packets をトレースできます。 **show platform hardware fed switch switch-number forward interface interface-type interface-number** コマンドは、入力スイッチのすべてのスタックメンバの packet 転送情報を統合します。これを実現するために、*switch_num* 引数と *interface-number* 引数で指定されたスイッチ番号が入力スイッチの番号と一致していることを確認してください。

PCAP ファイルに格納されているキャプチャされた packet から特定の packet をトレースするには、**show platform hardware fed switch forward interface interface-type interface-number pcap pcap-file-name number packet-number data** コマンドを使用します。

例

次に、**show platform hardware fed switch {switch_num | active | standby } forward interface** コマンドの出力例を示します。

```
Device#show platform hardware fed switch active forward interface gigabitEthernet 1/0/35
0000.0022.0055 0000.0055.0066 ipv4 44.44.0.2 55.55.0.2 udp 1222 3333
```

Show forward is running in the background. After completion, syslog will be generated.

```
*Sep 24 05:57:36.614: %SHFWD-6-PACKET_TRACE_DONE: Switch 1 R0/0: fed: Packet Trace Complete:
Execute (show platform hardware fed switch <> forward last summary|detail)
*Sep 24 05:57:36.614: %SHFWD-6-PACKET_TRACE_FLOW_ID: Switch 1 R0/0: fed: Packet Trace Flow
id is 150323855361
```

Related Commands

コマンド	説明
monitor capture interface	接続ポイントおよびパケットフロー方向を指定して、モニタキャプチャポイントを設定します。
monitor capture start	トラフィックトレースポイントでパケットデータのバッファへのキャプチャを開始します。
monitor capture stop	トラフィックトレースポイントでパケットデータのキャプチャを停止します。
monitor capture export	キャプチャされた packet をバッファに保存します。 このコマンドは、 show forward で pcap の入力として使用できる flash: 内の PCAP ファイルにモニタキャプチャバッファをエクスポートするために使用します。

show platform hardware fed switch fwd-asic counters tla

転送 ASIC からのカウンタのレジスタ情報を表示するには、特権 EXEC モードで **show platform hardware fed switch fwd-asic counters tla** コマンドを使用します。

```
show platform hardware fed switch {switch_num | active | standby} fwd-asic counters tla tla_counter  
{detail | drop | statistics} [asic ASIC_num] output location:filename
```

Syntax Description

switch {switch_num active standby }	情報を表示するスイッチ。次のオプションがあります。 <ul style="list-style-type: none">• switch_num: スイッチの ID。• active: アクティブスイッチに関する情報を表示します。• standby: 存在する場合、スタンバイスイッチに関する情報を表示します。
---	--

tlatla_counter *tla_counter* は、次の 3 文字の頭字語 (TLA) カウンタのいずれかです。

- AQM: Active Queue Management (アクティブキュー管理)
 - ASE: ACL Search Engine (ACL 検索エンジン)
 - DPP: DopplerE Point to Point (DopplerE ポイントツーポイント)
 - EGR: Egress Global Resolution (出力グローバル解決)
 - EPF: Egress Port FIFO (出力ポート FIFO)
 - ESM: Egress Scheduler Module (出力スケジューラモジュール)
 - EQC: Egress Queue Controller (出力キューコントローラ)
 - FPE: Flexible Parser (フレキシブルパーサー)
 - FPS: Flexible Pipe Stage (フレキシブルパイプステージ)
 - FSE Fib Search Engine (Fib 検索エンジン)
 - IGR: Ingress Global Resolution (出力グローバル解決)
 - IPF: Ingress Port FIFO (入力ポート FIFO)
 - IQS: Ingress Queues and Scheduler (入力キューとスケジューラ)
 - MSC: Macsec Engine (Macsec エンジン)
 - NFL: Netflow
 - NIF: Network Interface (ネットワーク インターフェイス)
 - PBC: Packet Buffer Complex (パケットバッファ複合)
 - PIM: Protocol Independent Multicast (プロトコル独立マルチキャスト)
 - PLC: Policer (ポリサー)
 - RMU: Recirculation Multiplexer Unit (再循環マルチプレクサユニット)
 - RRE: Reassembly Engine (再構成エンジン)
 - RWE: Rewrite Engine (書き換えエンジン)
 - SEC: Security Engine (セキュリティエンジン)
 - SIF: Stack Interface (スタックインターフェイス)
 - SPQ: Supervisor Packet Queuing Engine (スーパーバイザ パケット キューイング エンジン)
 - SQS: Stack Queues And Scheduler (スタック キューとスケジューラ)
 - SUP: Supervisor Interface (スーパーバイザ インターフェイス)
-

show platform hardware fed switch fwd-asic counters tla

detail	ゼロ以外のカウンタのレジスタの内容をすべて表示します。
drop	ゼロ以外のドロップカウンタのレジスタの内容をすべての表示します。
statistics	ゼロ以外の統計カウンタのレジスタの内容をすべて表示します。
ascii <i>asic_num</i>	(任意) ASIC を指定します。
output <i>location:filename</i>	カウンタレジスタの内容をダンプする出力ファイルを指定します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.1	コマンド出力が、読み取り可能な表形式に変更されました。出力ファイルのサイズも、値がゼロのフィールドを出力しないことで削減されました。 change キーワードは推奨しません。

Usage Guidelines テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。



Note TLAによっては、これらのドロップまたは統計レジスタがないため、**ドロップ**または**統計**オプションの一部として表示するレジスタがない場合があります。このような場合は、[No <detail|drop|statistics> counters to display for tla <TLA_NAME>] というメッセージが表示され、出力ファイルは生成されません。

例

次に、**show platform hardware fed active fwd-asic counters tla aqm** コマンドの出力例を示します。

```
Device#show platform hardware fed active fwd-asic counters tla aqm detail output flash:aqm
command to get counters for tla AQM succeeded
Device#
Device# more flash:aqm
=====
```

asic	core	Register Name	Fields	value
0	0	AqmRepTransitUsageCnt[0][0]	totalCntHighMark	: 0x4
			transitWait4DoneHighMark	: 0x2
0	1	AqmRepTransitUsageCnt[0][0]	totalCntHighMark	: 0x2
			transitWait4DoneHighMark	: 0x2

asic	core	Register Name	Fields	value
0	0	AqmGlobalHardBufCnt[0][0]	highWaterMark	: 0x3

asic	core	Register Name	Fields	value
0	0	AqmRedQueueStats[0][673]	acceptByteCnt2	: 0x4e44e
			acceptFrameCnt2	: 0x5e1
0	0	AqmRedQueueStats[0][674]	acceptByteCnt1	: 0x88
			acceptByteCnt2	: 0xa7c
			acceptFrameCnt1	: 0x2
			acceptFrameCnt2	: 0x16
0	0	AqmRedQueueStats[0][676]	acceptByteCnt2	: 0xfbf06
			acceptFrameCnt2	: 0x2440
0	0	AqmRedQueueStats[0][677]	acceptByteCnt2	: 0xcc
			acceptFrameCnt2	: 0x3
0	0	AqmRedQueueStats[0][687]	acceptByteCnt2	: 0x2caea0
			acceptFrameCnt2	: 0xa836
0	0	AqmRedQueueStats[0][691]	acceptByteCnt2	: 0x2dc
			acceptFrameCnt2	: 0x6
0	0	AqmRedQueueStats[0][692]	acceptByteCnt2	: 0xc518
			acceptFrameCnt2	: 0x2e6

show platform hardware fed active fwd-asic resource tcam utilization

TCAM (Ternary Content Addressable Memory) の使用状況に関するハードウェア情報を表示するには、特権 EXEC モードで **show platform hardware fed active fwd-asic resource tcam utilization** コマンドを使用します。

show platform hardware fed active fwd-asic resource tcam utilization[*asic-number*]

Syntax Description	<i>asic-number</i>	ASIC 番号。有効な値の範囲は 0 ~ 7 です。
---------------------------	--------------------	----------------------------

Command Modes	特権 EXEC (#)
----------------------	-------------

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.2.1	このコマンドは Cisco IOS XE Amsterdam 17.2.1 よりも前のリリースで導入されました。

Usage Guidelines スタックカブルスイッチでは、このコマンドに **switch** キーワード、**show platform hardware fed switch active fwd-asic resource tcam utilization** があります。非スタックカブルスイッチでは、**switch** キーワードは使用できません。

例

次に、**show platform hardware fed active fwd-asic resource tcam utilization** コマンドの出力例を示します。

```
Device# show platform hardware fed active fwd-asic resource tcam utilization
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable

CAM Utilization for ASIC [0]
Table          Subtype   Dir    Max    Used   %Used   V4     V6
MPLS   Other
-----
OPENFLOW Table0      TCAM     I    5000     5     0%     3     0
      0      2
OPENFLOW Table0 Ext. EM        I    8192     3     0%     0     0
      0      3
OPENFLOW Table1      TCAM     I    3600     1     0%     1     0
      0      0
OPENFLOW Table1 Ext. EM        I    8192     1     0%     0     0
      0      1
OPENFLOW Table2      TCAM     I    3500     1     0%     1     0
      0      0
OPENFLOW Table2 Ext. EM        I    8192     1     0%     0     0
      0      1
```

```

OPENFLOW Table3 Ext.  EM          I          8192      0      0%      0      0
0                    0
OPENFLOW Table4 Ext.  EM          I          8192      0      0%      0      0
0                    0
OPENFLOW Table5 Ext.  EM          I          8192      0      0%      0      0
0                    0
OPENFLOW Table6 Ext.  EM          I          8192      0      0%      0      0
0                    0
OPENFLOW Table7 Ext.  EM          I          8192      0      0%      0      0
0                    0
    
```

下の表に、ディスプレイ内に表示される重要なフィールドのリストを示します。

Table 18: show platform hardware fed active fwd-asic resource tcam utilization フィールドの説明

フィールド	説明
Table	OpenFlow テーブル番号。
Subtype	使用可能なサブタイプにはどのようなものがありますか？
Dir	
Max	
Used	
%Used	
V4	
V6	
MPLS	
Other	

show platform resources

プラットフォームのリソース情報を表示するには、特権 EXEC モードで **show platform resources** コマンドを使用します。

show platform resources

このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドの出力には、総メモリから正確な空きメモリを引いた値である使用メモリが表示されます。

例

次に、**show platform resources** コマンドの出力例を示します。

```
Switch# show platform resources

**State Acronym: H - Healthy, W - Warning, C - Critical

Resource Usage Max Warning Critical
State
-----
Control Processor 7.20% 100% 90% 95%
H
DRAM 2701MB (69%) 3883MB 90% 95%
H
```

show platform software audit

SE Linux 監査ログを表示するには、特権 EXEC モードで **show platform software audit** コマンドを使用します。

```
show platform software audit {all | summary | [switch {switch-number | active | standby}]
{0 | F0 | R0 | {FP | RP} {active}}}
```

Syntax Description	all	すべてのスロットからの監査ログを表示します。
	summary	すべてのスロットからの監査ログの要約カウントを表示します。
	switch	特定のスイッチのスロットについての監査ログを表示します。
	switch-number	指定したスイッチ番号のスイッチを選択します。
	switch active	スイッチのアクティブインスタンスを選択します。
	standby	スイッチのスタンバイインスタンスを選択します。
	0	SPA インターフェイス プロセッサ スロット 0 の監査ログを表示します。
	F0	Embedded-Service-Processor スロット 0 の監査ログを表示します。
	R0	Route-Processor スロット 0 の監査ログを表示します。
	FP active	アクティブな Embedded-Service-Processor スロットの監査ログを表示します。
	RP active	アクティブな Route-Processor スロットの監査ログを表示します。

Command Modes 特権 EXEC (#)

Command History

Usage Guidelines このコマンドは、Cisco IOS XE Gibraltar 16.10.1 で SELinux 許可モード機能の一部として導入されました。 **show platform software audit** コマンドは、アクセス違反イベントを含むシステム ログを表示します。

Cisco IOS XE Gibraltar 16.10.1 では、許可モードでの操作は、IOS XE プラットフォームの特定のコンポーネント（プロセスまたはアプリケーション）を制限する目的で利用できます。許可モードでは、アクセス違反イベントが検出され、システムログが生成されますが、イベントまたは操作自体はブロックされません。このソリューションは、主にアクセス違反検出モードで動作します。

次に、**show software platform software audit summary** コマンドの出力例を示します。

```
Device# show software platform software audit summary
```

```
=====
AUDIT LOG ON switch 1
-----
AVC Denial count: 58
=====
```

次に、**show software platform software audit all** コマンドの出力例を示します。

```
Device# show software platform software audit all
```

```
=====
AUDIT LOG ON switch 1
-----
===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc: denied { execute } for pid=8300 comm="sh"
name="id" dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438600.897:120): avc: denied { execute_no_trans } for pid=8300
comm="sh"
path="/tmp/sw/mount/cat9k-rpbase.2018-10-02_00.13_mhungund.SSA.pkg/nyquist/usr/bin/id"
dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438615.535:121): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
```

```
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539440246.697:149): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539440299.119:150): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====
```

次に、**show software platform software audit switch** コマンドの出力例を示します。

Device# **show platform software audit switch active R0**

```
===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
```

```
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====
```

show platform software fed switch punt cpuq rates

パントされたパスにおけるドロップを含むパケットのパントレートを表示するには、特権 EXEC モードで `show platform software fed switch punt cpuq rates` コマンドを使用します。

`show platform software fed switch {switch-number | active | standby} punt cpuq rates`

Syntax Description

`switch`{*switch-number* | **active** | **standby**}

スイッチに関する情報を表示します。次の選択肢があります。

- *switch-number*。
- **active** : アクティブなスイッチに関する情報を表示します。
- **standby**: 存在する場合、スタンバイスイッチに関する情報を表示します。

Note このキーワードはサポートされていません。

punt

パント情報を指定します。

cpuq

CPU受信キューに関する情報を指定します。

rates

パケットのパントレートを指定します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines

このコマンドの出力には、10 秒、1 分、5 分の各間隔のレートが 1 秒あたりのパケット数で表示されます。

例

次に、`show platform software fed switch active punt cpuq rates` コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq rates
```

```
Punt Rate CPU Q Statistics
```

```
Packets per second averaged over 10 seconds, 1 min and 5 mins
```

```
=====
```

Q	Queue	Rx	Rx	Rx	Drop	Drop	Drop

show platform software fed switch punt cpuq rates

no	Name	10s	1min	5min	10s	1min	5min
0	CPU_Q_DOT1X_AUTH	0	0	0	0	0	0
1	CPU_Q_L2_CONTROL	0	0	0	0	0	0
2	CPU_Q_FORUS_TRAFFIC	336	266	320	0	0	0
3	CPU_Q_ICMP_GEN	0	0	0	0	0	0
4	CPU_Q_ROUTING_CONTROL	0	0	0	0	0	0
5	CPU_Q_FORUS_ADDR_RESOLUTION	0	0	0	0	0	0
6	CPU_Q_ICMP_REDIRECT	0	0	0	0	0	0
7	CPU_Q_INTER_FED_TRAFFIC	0	0	0	0	0	0
8	CPU_Q_L2LVX_CONTROL_PKT	0	0	0	0	0	0
9	CPU_Q_EWLC_CONTROL	0	0	0	0	0	0
10	CPU_Q_EWLC_DATA	0	0	0	0	0	0
11	CPU_Q_L2LVX_DATA_PKT	0	0	0	0	0	0
12	CPU_Q_BROADCAST	0	0	0	0	0	0
13	CPU_Q_LEARNING_CACHE_OVFL	0	0	0	0	0	0
14	CPU_Q_SW_FORWARDING	0	0	0	0	0	0
15	CPU_Q_TOPOLOGY_CONTROL	0	0	0	0	0	0
16	CPU_Q_PROTO_SNOOPING	0	0	0	0	0	0
17	CPU_Q_DHCP_SNOOPING	0	0	0	0	0	0
18	CPU_Q_TRANSIT_TRAFFIC	0	0	0	0	0	0
19	CPU_Q_RPF_FAILED	0	0	0	0	0	0
20	CPU_Q_MCAST_END_STATION_SERVICE	0	0	0	0	0	0
21	CPU_Q_LOGGING	0	0	0	0	0	0
22	CPU_Q_PUNT_WEBAUTH	0	0	0	0	0	0
23	CPU_Q_HIGH_RATE_APP	0	0	0	0	0	0
24	CPU_Q_EXCEPTION	0	0	0	0	0	0
25	CPU_Q_SYSTEM_CRITICAL	0	0	0	0	0	0
26	CPU_Q_NFL_SAMPLED_DATA	0	0	0	0	0	0
27	CPU_Q_LOW_LATENCY	0	0	0	0	0	0
28	CPU_Q_EGR_EXCEPTION	0	0	0	0	0	0
29	CPU_Q_FSS	0	0	0	0	0	0
30	CPU_Q_MCAST_DATA	0	0	0	0	0	0
31	CPU_Q_GOLD_PKT	0	0	0	0	0	0

次の表で、この出力に表示される重要なフィールドを説明します。

Table 19: show platform software fed switch active punt cpuq rates フィールドの説明

フィールド	説明
Queue Name	キューの名前。
Rx	1秒あたりのパケットの受信レート（10秒、1分、5分）。
Drop	1秒あたりのパケットのドロップレート（10秒、1分、5分）。

show platform software fed switch punt packet-capture display

CPU 使用率が高いときの packets キャプチャ情報を表示するには、特権 EXEC モードで **show platform software fed switch active punt packet-capture display** コマンドを使用します。

show platform software fed switch active punt packet-capture display { detailed | hexdump }

Syntax Description	switch {switch-number active standby}	スイッチに関する情報を表示します。次の選択肢があります。
	<ul style="list-style-type: none"> active : アクティブなスイッチに関する情報を表示します。 standby : 存在する場合、スタンバイスイッチに関する情報を表示します。 <p>Note standby キーワードはサポートされていません。</p>	
	punt	パント情報を指定します。
	packet-capture display	キャプチャされたパケットに関する情報を指定します。
	detailed	キャプチャされたパケットに関する詳細な情報を指定します。
	hex-dump	キャプチャされたパケットに関する 16 進数形式の情報を指定します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines このコマンドの出力には、CPU 使用率が上限しきい値を超えているときの CPU バウンドパケット、インバンド CPU トラフィックレート、および実行中の CPU プロセスに関する定期的なログと永続的なログが表示されます。

Examples 次に、**show platform software fed switch active punt packet-capture display detailed** コマンドの出力例を示します。

```
Device# show platform software fed switch active punt packet-capture display detailed
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 101 packets. Capture capacity : 4096 packets
```

show platform software fed switch punt packet-capture display

```
----- Packet Number: 1, Timestamp: 2018/09/04 23:22:10.179 -----
interface : GigabitEthernet2/0/2 [if-id: 0x00000032] (physical)
ether hdr : dest mac: 0100.0ccc.cccd, src mac: 2c36.f8fc.4884
ether hdr : ethertype: 0x0032

Doppler Frame Descriptor :
  0000000044004E04 C00F402D94510000 0000000000000100 0000400401000000
  0000000001000050 000000006D000100 0000000025836200 0000000000000000

Packet Data Dump (length: 68 bytes) :
  01000CCCCCD2C36 F8FC48840032AAAA 0300000C010B0000 00000080012C36F8
  FC48800000000080 012C36F8FC488080 040000140002000F 0071000000020001
  244E733E

----- Packet Number: 2, Timestamp: 2018/09/04 23:22:10.179 -----
interface : GigabitEthernet2/0/2 [if-id: 0x00000032] (physical)
ether hdr : dest mac: 0180.c200.0000, src mac: 2c36.f8fc.4884
ether hdr : ethertype: 0x0026
!
!
!
```

show platform software fed switch punt rates interfaces

すべてのインターフェイスのパントレートの全体的な統計を表示するには、特権 EXEC モードで **show platform software fed switch punt rates interfaces** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby**} **punt rates interfaces**[*interface-id*]

Syntax Description	switch { <i>switch-number</i> active standby }	スイッチに関する情報を表示します。次の選択肢があります。 <ul style="list-style-type: none"> • <i>switch-number</i>。 • active : アクティブなスイッチに関する情報を表示します。 • standby: 存在する場合、スタンバイスイッチに関する情報を表示します。 <p>Note このキーワードはサポートされていません。</p>
	punt	パント情報を指定します。
	rates	パケットのパントレートを指定します。
	interfaces [<i>interface-id</i>]	(任意) インターフェイスの全体的な統計に加え、インターフェイスの 10 秒間隔でのキュー単位の設定を表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines この出力には、10 秒、1 分、5 分の各間隔のパントレートが 1 秒あたりのパケット数で表示されます。

例

次に、すべてのインターフェイスについての **show platform software fed switch active punt rates interfaces** コマンドの出力例を示します。

```
Device#show plataform software fed switch active punt rates interfaces
Punt Rate on Interfaces Statistics
```

show platform software fed switch punt rates interfaces

Packets per second averaged over 10 seconds, 1 min and 5 mins

```

=====
Interface Name          | IF_ID | Rx | Rx | Rx | Drop | Drop | Drop
                       |       | 10s | 1min | 5min | 10s | 1min | 5min
=====
Vlan3                   | 0x00000034 | 1000 | 1000 | 520 | 0 | 0 | 0
=====
    
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 20: show platform software fed switch active punt rates interfaces のフィールドの説明

フィールド	説明
Interface Name	物理インターフェイスの名前。
IF_ID	物理インターフェイスの ID。
Rx	1 秒あたりのパケットの受信レート（10 秒、1 分、5 分）。
Drop	1 秒あたりのパケットのドロップレート（10 秒、1 分、5 分）。

次に、特定のインターフェイスについての **show platform software fed switch active punt rates interfaces interface-id** コマンドの出力例を示します。

```

Device#show platform software fed switch active punt rates interfaces 0x31
Punt Rate on Single Interfaces Statistics
    
```

```

Interface : Port-channell1 [if_id: 0x31]
    
```

Received		Dropped	
-----		-----	
Total	: 29617	Total	: 0
10 sec average	: 0	10 sec average	: 0
1 min average	: 0	1 min average	: 0
5 min average	: 0	5 min average	: 0

Per CPUQ punt stats on the interface (rate averaged over 10s interval)

```

=====
Q | Queue | Recv | Recv | Drop | Drop |
no | Name | Total | Rate | Total | Rate |
=====
0 CPU_Q_DOT1X_AUTH 0 0 0 0
1 CPU_Q_L2_CONTROL 29519 0 0 0
2 CPU_Q_FORUS_TRAFFIC 0 0 0 0
3 CPU_Q_ICMP_GEN 0 0 0 0
4 CPU_Q_ROUTING_CONTROL 0 0 0 0
5 CPU_Q_FORUS_ADDR_RESOLUTION 0 0 0 0
6 CPU_Q_ICMP_REDIRECT 0 0 0 0
7 CPU_Q_INTER_FED_TRAFFIC 0 0 0 0
8 CPU_Q_L2LVX_CONTROL_PKT 0 0 0 0
9 CPU_Q_EWLC_CONTROL 0 0 0 0
10 CPU_Q_EWLC_DATA 0 0 0 0
11 CPU_Q_L2LVX_DATA_PKT 0 0 0 0
12 CPU_Q_BROADCAST 0 0 0 0
    
```

```

13 CPU_Q_LEARNING_CACHE_OVFL          0      0      0      0
14 CPU_Q_SW_FORWARDING                0      0      0      0
15 CPU_Q_TOPOLOGY_CONTROL             98      0      0      0
16 CPU_Q_PROTO_SNOOPING               0      0      0      0
17 CPU_Q_DHCP_SNOOPING                 0      0      0      0
18 CPU_Q_TRANSIT_TRAFFIC               0      0      0      0
19 CPU_Q_RPF_FAILED                    0      0      0      0
20 CPU_Q_MCAST_END_STATION_SERVICE    0      0      0      0
21 CPU_Q_LOGGING                       0      0      0      0
22 CPU_Q_PUNT_WEBAUTH                  0      0      0      0
23 CPU_Q_HIGH_RATE_APP                  0      0      0      0
24 CPU_Q_EXCEPTION                      0      0      0      0
25 CPU_Q_SYSTEM_CRITICAL                0      0      0      0
26 CPU_Q_NFL_SAMPLED_DATA              0      0      0      0
27 CPU_Q_LOW_LATENCY                   0      0      0      0
28 CPU_Q_EGR_EXCEPTION                 0      0      0      0
29 CPU_Q_FSS                            0      0      0      0
30 CPU_Q_MCAST_DATA                     0      0      0      0
31 CPU_Q_GOLD_PKT                       0      0      0      0
    
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 21: show platform software fed switch punt rates interfaces interface-id のフィールドの説明

フィールド	説明
Queue Name	キューの名前。
Recv Total	受信されたパケットの合計数。
Recv Rate	1秒あたりのパケットの受信レート。
Drop Total	破棄されたパケットの総数。
Drop Rate	1秒あたりのパケットのドロップレート。

show platform software ilpower

デバイス上のすべての PoE ポートのインラインパワーの詳細を表示するには、特権 EXEC モードで **show platform software ilpower** コマンドを使用します。

show platform software ilpower { **details** | **port** { **GigabitEthernet interface-number** } | **system slot-number** }

Syntax Description	details	port	GigabitEthernet interface-number	system slot-number
	すべてのインターフェイスのインラインパワーの詳細を表示します。	インラインパワー ポートの設定を表示します。	GigabitEthernet インターフェイス番号。値の範囲は0～9です。	インラインパワー システムの設定を表示します。

Command Modes	特権 EXEC (#)
---------------	-------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Examples

次に、**show platform software ilpower details** コマンドの出力例を示します。

```
Device# show platform software ilpower details
ILP Port Configuration for interface Gi1/0/1
  Initialization Done:  Yes
  ILP Supported:       Yes
  ILP Enabled:         Yes
  POST:                Yes
  Detect On:           No
  Powered Device Detected  No
  Powered Device Class Done  No
  Cisco Powered Device:   No
  Power is On:           No
  Power Denied:          No
  Powered Device Type:    Null
  Powerd Device Class:    Null
  Power State:           NULL
  Current State:         NGWC_ILP_DETECTING_S
  Previous State:        NGWC_ILP_SHUT_OFF_S
  Requested Power in milli watts:  0
  Short Circuit Detected:  0
  Short Circuit Count:    0
  Cisco Powerd Device Detect Count: 0
  Spare Pair mode:       0
  IEEE Detect:           Stopped
  IEEE Short:            Stopped
  Link Down:             Stopped
  Voltage sense:         Stopped
  Spare Pair Architecture: 1
```

```
Signal Pair Power allocation in milli watts: 0
Spare Pair Power On: 0
Powered Device power state: 0
Timer:
  Power Good: Stopped
  Power Denied: Stopped
  Cisco Powered Device Detect: Stopped
```

show platform software memory

指定したスイッチのメモリ情報を表示するには、特権 EXEC モードで **show platform software memory** コマンドを使用します。

show platform software memory [**chunk** | **database** | **messaging**] *process slot*

Syntax Description

Syntax Description

chunk	(任意) 指定したプロセスのチャンクメモリ情報を表示します。
database	(任意) 指定したプロセスのデータベースメモリ情報を表示します。
messaging	(任意) 指定したプロセスのメッセージングメモリ情報を表示します。 表示される情報は、内部デバッグのみを目的としています。

process

設定されているレベル。次のオプションがあります。

- **bt-logger**: Binary-Tracing Logger プロセス。
- **btrace-manager**: Btrace Manager プロセス。
- **chassis-manager**: Chassis Manager プロセス。
- **cli-agent**: CLI Agent プロセス。
- **cmm**: CMM プロセス。
- **dbm**: Database Manager プロセス。
- **dmiauthd**: DMI Authentication Daemon プロセス。
- **emd**: Environmental Monitoring プロセス。
- **fed**: Forwarding Engine Driver プロセス。
- **forwarding-manager**: Forwarding Manager プロセス。
- **geo**: Geo Manager プロセス。
- **gnmi**: GNMI プロセス。
- **host-manager**: Host Manager プロセス。
- **interface-manager**: Interface Manager プロセス。
- **iomd**: Input/Output Module daemon (IOMd) プロセス。
- **ios**: IOS プロセス。
- **iox-manager**: IOx Manager プロセス。
- **license-manager**: License Manager プロセス。
- **logger**: Logging Manager プロセス。
- **mdt-pubd**: Model Defined Telemetry Publisher プロセス。
- **ndbman**: Netconf DataBase Manager プロセス。
- **nesd**: Network Element Synchronizer Daemon プロセス。
- **nginx**: Nginx Webserver プロセス。
- **nif_mgr**: NIF Manager プロセス。
- **platform-mgr**: Platform Manager プロセス。
- **pluggable-services**: Pluggable Services プロセス。
- **replication-mgr**: Replication Manager プロセス。
- **shell-manager**: Shell Manager プロセス。

- **sif**: Stack Interface (SIF) Manager プロセス。
 - **smd**: Session Manager プロセス。
 - **stack-mgr**: Stack Manager プロセス。
 - **syncfd**: SyncmDaemon プロセス。
 - **table-manager**: Table Manager サーバ。
 - **thread-test**: Multithread Manager プロセス。
 - **virt-manager**: Virtualization Manager プロセス。
-

slot レベルが設定されているプロセスを実行中のハードウェアスロット。次のオプションがあります。

- **number:** レベルが設定されているハードウェアモジュールの SIP スロット番号。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
- **SIP-slot/SPA-bay:** SIP スイッチ スロットの数とその SIP の共有ポートアダプタ (SPA) ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
- **F0:** Embedded Service Processor スロット 0。
- **FP active:** アクティブな Embedded Service Processor。
- **R0:** スロット 0 のルート プロセッサ。
- **RP active:** アクティブなルート プロセッサ。
- **RP standby:** スタンバイのルート プロセッサ。
- **switch <number>:** 指定された番号を持つスイッチ。
- **switch active:** アクティブなスイッチ。
- **switch standby:** スタンバイスイッチ。
- **number:** レベルが設定されているハードウェアモジュールの SIP スロット番号。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
- **SIP-slot/SPA-bay:** SIP スイッチ スロットの数とその SIP の共有ポートアダプタ (SPA) ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
- **F0:** スロット 0 の Embedded Service Processor。
- **FP active:** アクティブな Embedded Service Processor。
- **R0:** スロット 0 のルート プロセッサ。
- **RP active:** アクティブなルート プロセッサ。

Command Default

デフォルトの動作や値はありません。

Command Modes

特権 EXEC (#)

Command History

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドを実行した。

次に、Cisco Catalyst 9000 シリーズ ESP スロット 0 の Forwarding Manager プロセスについての簡略化した形式（brief キーワード）のメモリ情報を表示する出力例を示します。

Device# show platform software memory forwarding-manager switch 1 fp active brief

module	allocated	requested	allocs	frees
Summary	5702540	5619788	121888	116716
AOM object	1920374	1920310	4	0
AOM links array	880379	880315	4	0
smc_message	819575	819511	4	0
AOM update state	640380	640316	4	0
dpidb-config	208776	203544	351	24
fman-infra-avl	178016	153680	1521	0
AOM batch	152373	152309	4	0
AOM asynchronous conte	128388	128324	4	0
AOM basic data	124824	124760	5	1
eventutil	118939	118299	50	10
AOM tree node	96465	96385	5	0
AOM tree root	72377	72313	4	0
acl	36090	31914	504	243
fman-infra-ipc	35326	24366	115097	114412
AOM uplink update node	32386	32322	4	0
unknown	30528	23808	424	4
uipeer	27232	27152	5	0
fman-infra-qos	26872	24712	164	29
cce-class	19427	15411	251	0
l2 control protocol	15472	12896	325	164
fman-infra-cce	15272	13576	106	0
smc_channel	15223	15159	4	0
unknown	14208	8736	447	105
chunk	12513	12033	33	3
cce-bind	8496	7552	82	23
MATM mac entry	8040	5928	544	412
adj	7064	6312	157	110
route-pfx	6116	5412	157	113
Filter_rules	4912	4896	1	0
fman-infra-dpidb	4130	2338	112	0
SMC Buffer	3794	3202	43	6
urpf-list	3028	2100	85	27
lookup	2480	2160	30	10
MATM mac table	2432	1600	148	96
cdllib	1688	1672	1	0
route-tbl	1600	1264	21	0
FNF Flowdef	1492	1460	3	1
acl-ref	1120	1024	8	2
cgm-lib	1120	880	410	395
pbr_if_cfg	1088	976	205	198
FNF Monitor	1048	1032	1	0
pbr_routemap	960	864	18	12
!				
!				
!				

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 22: show platform software memory briefのフィールドの説明

フィールド	説明
module	サブモジュールの名前。
allocated	割り当て済みのメモリ（バイト数）。
requested	アプリケーションによって要求されたバイト数。
allocs	個別の割り当てイベントの試行回数。
frees	解放イベントの数。

show platform software process list

プラットフォームで実行中のプロセスのリストを表示するには、特権 EXEC モードで **show platform software process list** コマンドを使用します。

show platform software process list switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**} [**name** *process-name* | **process-id** *process-ID* | **sort** **memory** | **summary**]

Syntax Description	
switch <i>switch-number</i>	スイッチに関する情報を表示します。 <i>switch-number</i> 引数の有効な値は 0 ~ 9 です。
active	スイッチのアクティブ インスタンスに関する情報を表示します。
standby	スイッチのスタンバイ インスタンスに関する情報を表示します。
0	共有ポート アダプタ (SPA) インターフェイス プロセッサ スロット 0 に関する情報を表示します。
F0	Embedded Service Processor (ESP) スロット 0 に関する情報を表示します。
R0	ルート プロセッサ (RP) スロット 0 に関する情報を表示します。
name <i>process-name</i>	(任意) 指定されたプロセスに関する情報を表示します。プロセス名を入力します。
process-id <i>process-ID</i>	(任意) 指定されたプロセス ID に関する情報を表示します。プロセス ID を入力します。
sort	(任意) プロセスに従いソートされた情報を表示します。
memory	(任意) メモリに従いソートされた情報を表示します。
summary	(任意) ホスト デバイスのプロセス メモリのサマリーを表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Examples

次に、**show platform software process list switch active R0** コマンドの出力例を示します。

```
Switch# show platform software process list switch active R0 summary
Total number of processes: 278
Running           : 2
Sleeping          : 276
Disk sleeping     : 0
Zombies           : 0
```

show platform software process list

```

Stopped          : 0
Paging           : 0

Up time          : 8318
Idle time        : 0
User time        : 216809
Kernel time      : 78931

Virtual memory   : 12933324800
Pages resident   : 634061
Major page faults: 2228
Minor page faults: 3491744

Architecture     : mips64
Memory (kB)
  Physical        : 3976852
  Total           : 3976852
  Used            : 2766952
  Free            : 1209900
  Active          : 2141344
  Inactive        : 1589672
  Inact-dirty     : 0
  Inact-clean     : 0
  Dirty           : 4
  AnonPages       : 1306800
  Bounce          : 0
  Cached          : 1984688
  Commit Limit    : 1988424
  Committed As    : 3358528
  High Total      : 0
  High Free       : 0
  Low Total       : 3976852
  Low Free        : 1209900
  Mapped          : 520528
  NFS Unstable    : 0
  Page Tables     : 17328
  Slab            : 0
  VMmalloc Chunk  : 1069542588
  VMmalloc Total  : 1069547512
  VMmalloc Used   : 2588
  Writeback       : 0
  HugePages Total: 0
  HugePages Free  : 0
  HugePages Rsvd  : 0
  HugePage Size   : 2048

Swap (kB)
  Total           : 0
  Used            : 0
  Free            : 0
  Cached          : 0

Buffers (kB)     : 439528

Load Average
  1-Min          : 1.13
  5-Min          : 1.18
  15-Min         : 0.92

```

次に、**show platform software process list switch active R0** コマンドの出力例を示します。

```

デバイス# show platform software process list switch active R0
Name                Pid    PPid  Group Id  Status  Priority  Size
-----
systemd             1      0      1  S        20    4876
kthreadd            2      0      0  S        20     0
ksoftirqd/0        3      2      0  S        20     0
kworker/0:0H       5      2      0  S         0     0
rcu_sched           7      2      0  S        20     0
rcu_bh              8      2      0  S        20     0
migration/0        9      2      0  S      4294967196 0
watchdog/0        10     2      0  S      4294967196 0
watchdog/1        11     2      0  S      4294967196 0
migration/1       12     2      0  S      4294967196 0
ksoftirqd/1       13     2      0  S        20     0
kworker/1:0H      15     2      0  S         0     0
watchdog/2        16     2      0  S      4294967196 0
migration/2       17     2      0  S      4294967196 0
ksoftirqd/2       18     2      0  S        20     0
kworker/2:0H      20     2      0  S         0     0
watchdog/3        21     2      0  S      4294967196 0
migration/3       22     2      0  S      4294967196 0
ksoftirqd/3       23     2      0  S        20     0
kworker/3:0       24     2      0  S        20     0
kworker/3:0H      25     2      0  S         0     0
kdevtmpfs          26     2      0  S        20     0
netns               27     2      0  S         0     0
perf                28     2      0  S         0     0
khungtaskd         29     2      0  S        20     0
writeback           30     2      0  S         0     0
ksmd                31     2      0  S        25     0
khugepaged          32     2      0  S        39     0
crypto              33     2      0  S         0     0
bioreset            34     2      0  S         0     0
kblockd             35     2      0  S         0     0
ata_sff             36     2      0  S         0     0
rpciod              37     2      0  S         0     0
kswapd0             63     2      0  S        20     0
vmstat              64     2      0  S         0     0
fsnotify_mark      65     2      0  S        20     0
nfsiod              66     2      0  S         0     0
.
.
.
    
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 23: show platform software process list のフィールドの説明

フィールド	説明
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。
Pid	プロセスを識別して追跡するためにオペレーティングシステムで使用されるプロセス ID が表示されます。

フィールド	説明
PPID	親プロセスのプロセス ID が表示されます。
Group Id	グループ ID が表示されます。
Status	人間が判読可能な形式でプロセスのステータスが表示されます。
Priority	無効にされたスケジューリングの優先順位が表示されます。
Size	Cisco IOS XE Gibraltar 16.10.1 よりも前: 仮想メモリのサイズが表示されます。 Cisco IOS XE Gibraltar 16.10.1 以降: RAM でそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ (RSS) が表示されます。

show platform software process memory

各システムプロセスで使用されているメモリの量を表示するには、特権 EXEC モードで **show platform software process memory** コマンドを使用します。

show platform process memory

```
switch { switch-number | active | standby } { 0 | F0 | FP | R0 } { all [sorted | virtual [sorted]] | name process-name { maps | smaps [summary] } | process-id process-id { maps | smaps [summary] } }
```

Syntax Description

switch <i>switch-number</i>	スイッチに関する情報を表示します。スイッチ番号を入力します。
active	デバイスのアクティブインスタンスを指定します。
standby	デバイスのスタンバイインスタンスを指定します。
0	共有ポートアダプタ (SPA) インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor (ESP) スロット 0 を指定します。
FP	Embedded Service Processor (ESP) を指定します。
R0	ルートプロセッサ (RP) スロット 0 を指定します。
all	すべてのプロセスを一覧表示します。
sorted	(任意) 常駐セットサイズ (RSS) に基づいて出力をソートします。
virtual	(任意) 仮想メモリを指定します。
name <i>process-name</i>	プロセス名を指定します。
maps	プロセスのメモリマップを指定します。
smaps summary	プロセスの smaps の要約を指定します。
process-id <i>process-id</i>	プロセス ID を指定します。

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Command Modes 特権 EXEC (#)

次に例を示します。

次に、**show platform software process memory active R0 all** コマンドの出力例を示します。

```
Device# show platform software process memory switch active R0 all
```

Pid	RSS	PSS	Heap	Shared	Private	Name
1	4876	3229	1064	1808	3068	systemd
118	3184	1327	132	2352	832	systemd-journal
159	3008	1191	396	1996	1012	systemd-udev
407	3192	1262	132	2196	996	dbus-daemon
3406	4772	3064	264	1940	2832	virtlogd
3411	5712	3474	2964	2344	3368	droputil.sh
3416	2588	358	132	2336	252	libvirtd.sh
3420	5708	3484	2976	2308	3400	reflector.sh
3424	1804	263	132	1632	172	xinetd
3425	964	118	132	872	92	sleep
3434	3060	844	528	2304	756	oom.sh
3442	2068	606	132	1604	464	rpcbind
3485	2380	845	132	1636	744	rpc.statd
3486	1632	338	132	1348	284	boothelper_evt.
3493	1136	156	132	1004	132	inotifywait
3504	2048	753	132	1372	676	rpc.mountd
3584	2868	620	36	2384	484	rotee
3649	1032	116	132	944	88	sleep
3705	2784	613	36	2296	488	rotee
3718	2856	610	36	2376	480	rotee
3759	1292	184	132	1136	156	inotifywait
3787	4256	2040	1640	2300	1956	iptbl.sh
3894	2948	637	36	2460	488	rotee
4017	1380	175	132	1236	144	inotifywait
4866	1820	287	132	1624	196	xinetd
5887	1692	257	132	1508	184	xinetd
5891	7248	4984	4584	2348	4900	rollback_timer.
5893	1764	257	132	1588	176	xinetd
6031	2804	601	36	2332	472	rotee
6037	1228	163	132	1092	136	inotifywait
6077	4736	3389	2992	1368	3368	psvp.sh
6115	1620	476	36	1152	468	rotee
6122	624	149	132	480	144	inotifywait
6127	5440	4077	3680	1384	4056	pvp.sh
6165	1736	592	36	1152	584	rotee
6245	624	149	132	480	144	inotifywait
6353	2592	1260	924	1352	1240	pman.sh
6470	1632	488	36	1152	480	rotee
6499	2588	1262	924	1348	1240	pman.sh
6666	1640	496	36	1152	488	rotee
6718	2584	1258	800	1348	1236	pman.sh
6736	8360	7020	6640	1360	7000	auto_upgrade_cl
6909	1636	492	36	1152	484	rotee
6955	2588	1262	928	1348	1240	pman.sh
7029	2196	679	40	1552	644	auto_upgrade_se
7149	1636	492	36	1152	484	rotee
7224	13200	4595	48	9368	3832	bt_logger
7295	2588	1262	800	1348	1240	pman.sh
.						
.						
.						

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 24: show platform software process memory のフィールドの説明

フィールド	説明
PID	プロセスを識別して追跡するためにオペレーティングシステムで使用されるプロセス ID が表示されます。
RSS	RAM でそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ（キロバイト（KB））が表示されます。
PSS	プロセスの比例セットサイズが表示されます。これは、メモリ内のページの数であり、各ページはそれを共有するプロセスの数で除算されます。
Heap	ユーザが割り当てたすべてのメモリの場所が表示されます。
Shared	共有クリーン+共有ダーティ
Private	プライベートクリーン+プライベートダーティ
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。

show platform software process slot switch

プラットフォーム ソフトウェア プロセスのスイッチ情報を表示するには、特権 EXEC モードで **show platform software process slot switch** コマンドを使用します。

show platform software process slot switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**}
monitor [*cycles no-of-times* [*interval delay* [*lines number*]]]

Syntax Description	
<i>switch-number</i>	スイッチ番号。
active	アクティブ インスタンスを指定します。
standby	スタンバイ インスタンスを指定します。
0	共有ポートアダプタ (SPA) インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor (ESP) スロット 0 を指定します。
R0	ルート プロセッサ (RP) スロット 0 を指定します。
monitor	実行中のプロセスをモニタします。
<i>cycles no-of-times</i>	(任意) monitor コマンドを実行する回数を設定します。有効な値は、1 ~ 4294967295 です。デフォルトは 5 です。
<i>interval delay</i>	(任意) それぞれの遅延を設定します。有効値は 0 ~ 300 です。デフォルトは 3 です。
<i>lines number</i>	(任意) 表示される出力の行数を設定します。有効値は 0 ~ 512 です。デフォルトは 0 です。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show platform software process slot switch** コマンドと **show processes cpu platform monitor location** コマンドの出力に、Linux **top** コマンドの出力が表示されます。これらのコマンドの出力には、**top** コマンドで表示される「空きメモリ」と「使用メモリ」が表示されます。これらのコマンドによって「空きメモリ」と「使用メモリ」に表示される値は、その他のプラットフォーム メモリ関連 CLI の出力で表示される値とは一致しません。

Examples

次に、**show platform software process slot monitor** コマンドの出力例を示します。

```
Switch# show platform software process slot switch active R0 monitor

top - 00:01:52 up 1 day, 11:20,  0 users,  load average: 0.50, 0.68, 0.83
Tasks: 311 total,  2 running, 309 sleeping,  0 stopped,  0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3955036k used,    21808k free,   419312k buffers
Swap:        0k total,        0k used,        0k free,   1946764k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  5693 root       20   0  3448 1368  912  R   7   0.0    0:00.07 top
 17546 root       20   0 2044m 244m  79m  S   7   6.3  186:49.08 fed main event
 18662 root       20   0 1806m 678m 263m  S   5  17.5  215:32.38 linux_iods-imag
 30276 root       20   0  171m  42m  33m  S   5   1.1  125:06.77 repm
 17835 root       20   0  935m  74m  63m  S   4   1.9   82:28.31 sif_mgr
 18534 root       20   0  182m 150m  10m  S   2   3.9    8:12.08 smand
    1 root       20   0  8440 4740 2184  S   0   0.1    0:09.52 systemd
    2 root       20   0    0    0    0  S   0   0.0    0:00.00 kthreadd
    3 root       20   0    0    0    0  S   0   0.0    0:02.86 ksoftirqd/0
    5 root        0 -20    0    0    0  S   0   0.0    0:00.00 kworker/0:0H
    7 root       RT    0    0    0    0  S   0   0.0    0:01.44 migration/0
    8 root       20   0    0    0    0  S   0   0.0    0:00.00 rcu_bh
    9 root       20   0    0    0    0  S   0   0.0    0:23.08 rcu_sched
   10 root       20   0    0    0    0  S   0   0.0    0:58.04 rcuc/0
   11 root       20   0    0    0    0  S   0   0.0   21:35.60 rcuc/1
   12 root       RT    0    0    0    0  S   0   0.0    0:01.33 migration/1
```

Related Commands

コマンド	説明
show processes cpu platform monitor location	IOS XE プロセスの CPU 使用率に関する情報を表示します。

show platform software status control-processor

プラットフォームソフトウェアの制御プロセッサのステータスを表示するには、特権 EXEC モードで **show platform software status control-processor** コマンドを使用します。

show platform software status control-processor [brief]

Syntax Description	brief (任意) プラットフォームの制御プロセッサのステータスのサマリーを表示します。				
Command Modes	特権 EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Examples

次に、**show platform memory software status control-processor** コマンドの出力例を示します。

```
Switch# show platform software status control-processor

2-RP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 1.00, status: healthy, under 5.00
  5-Min: 1.21, status: healthy, under 5.00
 15-Min: 0.90, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2766284 (70%), status: healthy
  Free: 1210568 (30%)
  Committed: 3358008 (84%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  4.40, System:  1.70, Nice:  0.00, Idle: 93.80
  IRQ:  0.00, SIRQ:  0.10, IOWait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  3.80, System:  1.20, Nice:  0.00, Idle: 94.90
  IRQ:  0.00, SIRQ:  0.10, IOWait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  7.00, System:  1.10, Nice:  0.00, Idle: 91.89
  IRQ:  0.00, SIRQ:  0.00, IOWait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  4.49, System:  0.69, Nice:  0.00, Idle: 94.80
  IRQ:  0.00, SIRQ:  0.00, IOWait:  0.00

3-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.24, status: healthy, under 5.00
  5-Min: 0.27, status: healthy, under 5.00
 15-Min: 0.32, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2706768 (68%), status: healthy
  Free: 1270084 (32%)
  Committed: 3299332 (83%), under 95%
Per-core Statistics
```

```
CPU0: CPU Utilization (percentage of time spent)
  User: 4.50, System: 1.20, Nice: 0.00, Idle: 94.20
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 5.20, System: 0.50, Nice: 0.00, Idle: 94.29
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 3.60, System: 0.70, Nice: 0.00, Idle: 95.69
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 3.00, System: 0.60, Nice: 0.00, Idle: 96.39
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

4-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.21, status: healthy, under 5.00
  5-Min: 0.24, status: healthy, under 5.00
 15-Min: 0.24, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1452404 (37%), status: healthy
  Free: 2524448 (63%)
  Committed: 1675120 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User: 2.30, System: 0.40, Nice: 0.00, Idle: 97.30
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 4.19, System: 0.69, Nice: 0.00, Idle: 95.10
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 4.79, System: 0.79, Nice: 0.00, Idle: 94.40
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 2.10, System: 0.40, Nice: 0.00, Idle: 97.50
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

9-RP0: unknown, statistics updated 4 seconds ago
Load Average: healthy
  1-Min: 0.20, status: healthy, under 5.00
  5-Min: 0.35, status: healthy, under 5.00
 15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1451328 (36%), status: healthy
  Free: 2525524 (64%)
  Committed: 1675932 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User: 1.90, System: 0.50, Nice: 0.00, Idle: 97.60
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 4.39, System: 0.19, Nice: 0.00, Idle: 95.40
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 5.70, System: 1.00, Nice: 0.00, Idle: 93.30
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 1.30, System: 0.60, Nice: 0.00, Idle: 98.00
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
```

次に、**show platform memory software status control-processor brief** コマンドの出力例を示します。

Switch# **show platform software status control-processor brief**

Load Average

Slot	Status	1-Min	5-Min	15-Min
2-RP0	Healthy	1.10	1.21	0.91
3-RP0	Healthy	0.23	0.27	0.31
4-RP0	Healthy	0.11	0.21	0.22
9-RP0	Healthy	0.10	0.30	0.34

Memory (kB)

Slot	Status	Total	Used (Pct)	Free (Pct)	Committed (Pct)
2-RP0	Healthy	3976852	2766956 (70%)	1209896 (30%)	3358352 (84%)
3-RP0	Healthy	3976852	2706824 (68%)	1270028 (32%)	3299276 (83%)
4-RP0	Healthy	3976852	1451888 (37%)	2524964 (63%)	1675076 (42%)
9-RP0	Healthy	3976852	1451580 (37%)	2525272 (63%)	1675952 (42%)

CPU Utilization

Slot	CPU	User	System	Nice	Idle	IRQ	SIRQ	IOWait
2-RP0	0	4.10	2.00	0.00	93.80	0.00	0.10	0.00
	1	4.60	1.00	0.00	94.30	0.00	0.10	0.00
	2	6.50	1.10	0.00	92.40	0.00	0.00	0.00
	3	5.59	1.19	0.00	93.20	0.00	0.00	0.00
3-RP0	0	2.80	1.20	0.00	95.90	0.00	0.10	0.00
	1	4.49	1.29	0.00	94.20	0.00	0.00	0.00
	2	5.30	1.60	0.00	93.10	0.00	0.00	0.00
	3	5.80	1.20	0.00	93.00	0.00	0.00	0.00
4-RP0	0	1.30	0.80	0.00	97.89	0.00	0.00	0.00
	1	1.30	0.20	0.00	98.50	0.00	0.00	0.00
	2	5.60	0.80	0.00	93.59	0.00	0.00	0.00
	3	5.09	0.19	0.00	94.70	0.00	0.00	0.00
9-RP0	0	3.99	0.69	0.00	95.30	0.00	0.00	0.00
	1	2.60	0.70	0.00	96.70	0.00	0.00	0.00
	2	4.49	0.89	0.00	94.60	0.00	0.00	0.00
	3	2.60	0.20	0.00	97.20	0.00	0.00	0.00

show platform software thread list

プラットフォームのスレッドのリストを表示するには、特権 EXEC モードで **show platform software thread list** コマンドを使用します。

show platform software thread list switch { *switch-number* | **active** | **standby** } { **0** | **F0** | **FP active** | **R0** } **pname** { **cdman** | **vidman** | **all** } **tname** { **main** | **pktio** | **rt** | **all** }

Syntax Description	switch <i>switch-number</i>	スイッチに関する情報を表示します。スイッチ番号を入力します。
	active	デバイスのアクティブインスタンスを指定します。
	standby	デバイスのスタンバイインスタンスを指定します。
	0	共有ポートアダプタ (SPA) インターフェイス プロセッサ スロット 0 を指定します。
	F0	Embedded Service Processor (ESP) スロット 0 を指定します。
	FP active	Embedded Service Processor (ESP) のアクティブインスタンスを指定します。
	R0	ルートプロセッサ (RP) スロット 0 を指定します。
	pname	プロセス名を指定します。指定できる値は cdman 、 vidman 、および all です。
	tname	スレッド名を指定します。指定できる値は main 、 pktio 、 rt 、および all です。

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Command Modes 特権 EXEC (#)

次に例を示します。

次に、**show platform software thread list switch active R0 pname cdman tname all** コマンドの出力例を示します。

show platform software thread list

```
Device# show platform software thread list switch active R0 pname cdman tname all
Name          Tid    PPid  Group Id  Core    Vcswch  Nvcswch  Status    Priority
TIME+  Size
-----
cdman         8407   7295   8407     1        0        0  S          20
12309  36976
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 25: show platform software thread list のフィールドの説明

フィールド	説明
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。
Tid	プロセス ID が表示されます。
PPid	親プロセスのプロセス ID が表示されます。
Group Id	グループ ID が表示されます。
Core	プロセッサ情報が表示されます。
Vcswch	自発的なコンテキストスイッチの回数が表示されます。
Nvcswch	非自発的なコンテキストスイッチの回数が表示されます。
Status	人間が判読可能な形式でプロセスのステータスが表示されます。
Priority	無効にされたスケジューリングの優先順位が表示されます。
TIME+	プロセスが開始されてからの経過時間が表示されます。
Size	RAM でそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ (キロバイト (KB)) が表示されます。

show processes cpu platform

IOS XE プロセスの CPU 使用率に関する情報を表示するには、特権 EXEC モードで **show processes cpu platform** コマンドを使用します。

show processes cpu platform [[**sorted** [**1min** | **5min** | **5sec**]] **location** **switch** { *switch-number* | **active** | **standby** } { **F0** | **FP active** | **R0** | **RP active** }

Syntax Description	
sorted	(任意) プラットフォームの CPU 使用率に基づいてソートした出力を表示します。
1min	(任意) 1 分間隔でソートします。
5min	(任意) 5 分間隔でソートします。
5sec	(任意) 5 秒間隔でソートします。
location	Field Replaceable Unit (FRU) の場所を指定します。
switch <i>switch-number</i>	スイッチに関する情報を表示します。スイッチ番号を入力します。
active	デバイスのアクティブインスタンスを指定します。
standby	デバイスのスタンバイインスタンスを指定します。
F0	Embedded Service Processor (ESP) スロット 0 を指定します。
FP active	Embedded Service Processor (ESP) のアクティブインスタンスを指定します。
R0	ルートプロセッサ (RP) スロット 0 を指定します。
RP active	ルートプロセッサ (RP) のアクティブインスタンスを指定します。

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Command Modes 特権 EXEC (#)

次に例を示します。

次に、**show processes cpu platform** コマンドの出力例を示します。

```
Device# show processes cpu platform
CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 2%
Core 0: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 2%
Core 1: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 2: CPU utilization for five seconds: 3%, one minute: 1%, five minutes: 1%
```

show processes cpu platform

```
Core 3: CPU utilization for five seconds: 2%, one minute: 5%, five minutes: 2%
  Pid  PPid  5Sec  1Min  5Min  Status  Size  Name
-----
    1     0   0%   0%   0%  S        4876  systemd
    2     0   0%   0%   0%  S         0  kthreadd
    3     2   0%   0%   0%  S         0  ksoftirqd/0
    5     2   0%   0%   0%  S         0  kworker/0:0H
    7     2   0%   0%   0%  S         0  rcu_sched
    8     2   0%   0%   0%  S         0  rcu_bh
    9     2   0%   0%   0%  S         0  migration/0
   10     2   0%   0%   0%  S         0  watchdog/0
   11     2   0%   0%   0%  S         0  watchdog/1
   12     2   0%   0%   0%  S         0  migration/1
   13     2   0%   0%   0%  S         0  ksoftirqd/1
   15     2   0%   0%   0%  S         0  kworker/1:0H
   16     2   0%   0%   0%  S         0  watchdog/2
   17     2   0%   0%   0%  S         0  migration/2
   18     2   0%   0%   0%  S         0  ksoftirqd/2
   20     2   0%   0%   0%  S         0  kworker/2:0H
   21     2   0%   0%   0%  S         0  watchdog/3
   22     2   0%   0%   0%  S         0  migration/3
   23     2   0%   0%   0%  S         0  ksoftirqd/3
   24     2   0%   0%   0%  S         0  kworker/3:0
   25     2   0%   0%   0%  S         0  kworker/3:0H
   26     2   0%   0%   0%  S         0  kdevtmpfs
   27     2   0%   0%   0%  S         0  netns
   28     2   0%   0%   0%  S         0  perf
   29     2   0%   0%   0%  S         0  khungtaskd
   30     2   0%   0%   0%  S         0  writeback
   31     2   7%   8%   8%  S         0  ksm
   32     2   0%   0%   0%  S         0  khugepaged
   33     2   0%   0%   0%  S         0  crypto
   34     2   0%   0%   0%  S         0  bioset
   35     2   0%   0%   0%  S         0  kblockd
   36     2   0%   0%   0%  S         0  ata_sff
   37     2   0%   0%   0%  S         0  rpciod
   63     2   0%   0%   0%  S         0  kswapd0
   64     2   0%   0%   0%  S         0  vmstat
   65     2   0%   0%   0%  S         0  fsnotify_mark
.
.
.
```

次に、 show processes cpu platform sorted 5min location switch 5 R0

```
Device# show processes cpu platform sorted 5min location switch 5 R0

CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 0: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 1: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 2: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 1%
Core 4: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 5: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 6: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 7: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
  Pid  PPid  5Sec  1Min  5Min  Status  Size  Name
-----
 16358 15516   4%   4%   4%  S    221376  fed main event
 14062 12756   1%   1%   1%  S     52140  sif_mgr
 32105  8618   0%   0%   0%  S         260  inotifywait
 31396 31393   0%   0%   0%  S     36516  python2.7
 31393 31271   0%   0%   0%  S     2744  rdope.sh
 31319   1    0%   0%   0%  S     2648  rotee
 31271   1    0%   0%   0%  S     3852  pman.sh
```

```

29671      2      0%      0%      0% S              0 kworker/u16:0
29341    29329      0%      0%      0% S             1780 sntp
29329      1      0%      0%      0% S             2788 stack_snntp.sh
.
.
.

```

次に、**show processes cpu platform location switch 7 R0** コマンドの出力例を示します。

```

Device# show processes cpu platform location switch 7 R0

CPU utilization for five seconds: 3%, one minute: 3%, five minutes: 3%
Core 0: CPU utilization for five seconds: 1%, one minute: 5%, five minutes: 5%
Core 1: CPU utilization for five seconds: 1%, one minute: 11%, five minutes: 5%
Core 2: CPU utilization for five seconds: 22%, one minute: 7%, five minutes: 6%
Core 3: CPU utilization for five seconds: 5%, one minute: 6%, five minutes: 6%
Core 4: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 5: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 6: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 7: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 6%

```

Pid	PPid	5Sec	1Min	5Min	Status	Size	Name
1	0	0%	0%	0%	S	8044	systemd
2	0	0%	0%	0%	S	0	kthreadd
.

show processes cpu platform history

システムの CPU 使用率の履歴に関する情報を表示するには、**show processes cpu platform history** コマンドを使用します。

show processes cpu platform history [**1min** | **5min** | **5sec** | **60min**] **location**
switch { *switch-number* | **active** | **standby** } { **0** | **F0** | **FP active** | **R0** }

1min	(任意) 1 分間隔の CPU 使用率の履歴を表示します。
5min	(任意) 5 分間隔の CPU 使用率の履歴を表示します。
5sec	(任意) 5 秒間隔の CPU 使用率の履歴を表示します。
60min	(任意) 60 分間隔の CPU 使用率の履歴を表示します。
location	Field Replaceable Unit (FRU) の場所を指定します。
switch <i>switch-number</i>	スイッチに関する情報を表示します。スイッチ番号を入力します。
active	デバイスのアクティブインスタンスを指定します。
standby	デバイスのスタンバイインスタンスを指定します。
0	共有ポートアダプタ (SPA) インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor (ESP) スロット 0 を指定します。
FP active	Embedded Service Processor (ESP) のアクティブインスタンスを指定します。
R0	ルートプロセッサ (RP) スロット 0 を指定します。

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Command Modes 特権 EXEC (#)

次に例を示します。

次に、**show processes cpu platform** コマンドの出力例を示します。

```
Device# show processes cpu platform

CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 2%
Core 0: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 2%
Core 1: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 2: CPU utilization for five seconds: 3%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 2%, one minute: 5%, five minutes: 2%
  Pid   PPid   5Sec   1Min   5Min   Status   Size   Name
-----
    1     0    0%    0%    0%    S         4876  systemd
    2     0    0%    0%    0%    S          0  kthreadd
    3     2    0%    0%    0%    S          0  ksoftirqd/0
    5     2    0%    0%    0%    S          0  kworker/0:0H
    7     2    0%    0%    0%    S          0  rcu_sched
    8     2    0%    0%    0%    S          0  rcu_bh
    9     2    0%    0%    0%    S          0  migration/0
   10     2    0%    0%    0%    S          0  watchdog/0
   11     2    0%    0%    0%    S          0  watchdog/1
   12     2    0%    0%    0%    S          0  migration/1
   13     2    0%    0%    0%    S          0  ksoftirqd/1
   15     2    0%    0%    0%    S          0  kworker/1:0H
   16     2    0%    0%    0%    S          0  watchdog/2
   17     2    0%    0%    0%    S          0  migration/2
   18     2    0%    0%    0%    S          0  ksoftirqd/2
   20     2    0%    0%    0%    S          0  kworker/2:0H
   21     2    0%    0%    0%    S          0  watchdog/3
   22     2    0%    0%    0%    S          0  migration/3
   23     2    0%    0%    0%    S          0  ksoftirqd/3
   24     2    0%    0%    0%    S          0  kworker/3:0
   25     2    0%    0%    0%    S          0  kworker/3:0H
   26     2    0%    0%    0%    S          0  kdevtmpfs
   27     2    0%    0%    0%    S          0  netns
   28     2    0%    0%    0%    S          0  perf
   29     2    0%    0%    0%    S          0  khungtaskd
   30     2    0%    0%    0%    S          0  writeback
   31     2    7%    8%    8%    S          0  ksmd
   32     2    0%    0%    0%    S          0  khugepaged
   33     2    0%    0%    0%    S          0  crypto
   34     2    0%    0%    0%    S          0  bioset
   35     2    0%    0%    0%    S          0  kblockd
   36     2    0%    0%    0%    S          0  ata_sff
   37     2    0%    0%    0%    S          0  rpciod
   63     2    0%    0%    0%    S          0  kswapd0
   64     2    0%    0%    0%    S          0  vmstat
   65     2    0%    0%    0%    S          0  fsnotify_mark
.
.
.
```

次に、**show processes cpu platform history 5sec** コマンドの出力例を示します。

```
Device# show processes cpu platform history 5sec

5 seconds ago, CPU utilization: 0%
10 seconds ago, CPU utilization: 0%
15 seconds ago, CPU utilization: 0%
20 seconds ago, CPU utilization: 0%
```

show processes cpu platform history

```
25 seconds ago, CPU utilization: 0%
30 seconds ago, CPU utilization: 0%
35 seconds ago, CPU utilization: 0%
40 seconds ago, CPU utilization: 0%
45 seconds ago, CPU utilization: 0%
50 seconds ago, CPU utilization: 0%
55 seconds ago, CPU utilization: 0%
60 seconds ago, CPU utilization: 0%
65 seconds ago, CPU utilization: 0%
70 seconds ago, CPU utilization: 0%
75 seconds ago, CPU utilization: 0%
80 seconds ago, CPU utilization: 0%
85 seconds ago, CPU utilization: 0%
90 seconds ago, CPU utilization: 0%
95 seconds ago, CPU utilization: 0%
100 seconds ago, CPU utilization: 0%
105 seconds ago, CPU utilization: 0%
110 seconds ago, CPU utilization: 0%
115 seconds ago, CPU utilization: 0%
120 seconds ago, CPU utilization: 0%
125 seconds ago, CPU utilization: 0%
130 seconds ago, CPU utilization: 0%
135 seconds ago, CPU utilization: 0%
140 seconds ago, CPU utilization: 0%
145 seconds ago, CPU utilization: 1%
150 seconds ago, CPU utilization: 0%
155 seconds ago, CPU utilization: 0%
160 seconds ago, CPU utilization: 0%
165 seconds ago, CPU utilization: 0%
170 seconds ago, CPU utilization: 0%
175 seconds ago, CPU utilization: 0%
180 seconds ago, CPU utilization: 0%
185 seconds ago, CPU utilization: 0%
190 seconds ago, CPU utilization: 0%
195 seconds ago, CPU utilization: 0%
200 seconds ago, CPU utilization: 0%
205 seconds ago, CPU utilization: 0%
210 seconds ago, CPU utilization: 0%
215 seconds ago, CPU utilization: 0%
220 seconds ago, CPU utilization: 0%
225 seconds ago, CPU utilization: 0%
230 seconds ago, CPU utilization: 0%
235 seconds ago, CPU utilization: 0%
240 seconds ago, CPU utilization: 0%
245 seconds ago, CPU utilization: 0%
250 seconds ago, CPU utilization: 0%
.
.
.
```

show processes cpu platform monitor

IOS XE プロセスの CPU 使用率に関する情報を表示するには、特権 EXEC モードで **show processes cpu platform monitor** コマンドを使用します。

show processes cpu platform monitor location switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**}

Syntax Description	location	Field Replaceable Unit (FRU) の場所に関する情報を表示します。
	switch	スイッチを指定します。
	<i>switch-number</i>	スイッチ番号。
	active	アクティブ インスタンスを指定します。
	standby	スタンバイ インスタンスを指定します。
	0	共有ポートアダプタ (SPA) インターフェイス プロセッサ スロット 0 を指定します。
	F0	Embedded Service Processor (ESP) スロット 0 を指定します。
	R0	ルート プロセッサ (RP) スロット 0 を指定します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show platform software process slot switch** コマンドと **show processes cpu platform monitor location** コマンドの出力に、Linux **top** コマンドの出力が表示されます。これらのコマンドの出力には、**top** コマンドで表示される「空きメモリ」と「使用メモリ」が表示されます。これらのコマンドによって「空きメモリ」と「使用メモリ」に表示される値は、その他のプラットフォーム メモリ関連 CLI の出力で表示される値とは一致しません。

Examples

次に、**show processes cpu monitor location switch active R0** コマンドの出力例を示します。

```
Switch# show processes cpu platform monitor location switch active R0

top - 00:04:21 up 1 day, 11:22, 0 users, load average: 0.42, 0.60, 0.78
Tasks: 312 total, 4 running, 308 sleeping, 0 stopped, 0 zombie
Cpu(s): 7.4%us, 3.3%sy, 0.0%ni, 89.2%id, 0.0%wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 3976844k total, 3956928k used, 19916k free, 419312k buffers
Swap: 0k total, 0k used, 0k free, 1947036k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  6294 root        20   0 3448 1368  912  R   9.0   0.0   0:00.07 top
```

show processes cpu platform monitor

```

17546 root      20    0 2044m 244m   79m S    7   6.3 187:02.07 fed main event
30276 root      20    0  171m  42m   33m S    7   1.1 125:15.54 repm
   16 root      20    0    0    0    0 S    5   0.0  22:07.92 rcuc/2
   21 root      20    0    0    0    0 R    5   0.0  22:13.24 rcuc/3
18662 root      20    0 1806m 678m  263m R    5  17.5 215:47.59 linux_iosd-imag
   11 root      20    0    0    0    0 S    4   0.0  21:37.41 rcuc/1
10333 root      20    0  6420 3916 1492 S    4   0.1   4:47.03 btrace_rotate.s
   10 root      20    0    0    0    0 S    2   0.0   0:58.13 rcuc/0
  6304 root      20    0   776  12    0 R    2   0.0   0:00.01 ls
17835 root      20    0  935m  74m   63m S    2   1.9  82:34.07 sif_mgr
   1 root      20    0  8440 4740 2184 S    0   0.1   0:09.52 systemd
   2 root      20    0    0    0    0 S    0   0.0   0:00.00 kthreadd
   3 root      20    0    0    0    0 S    0   0.0   0:02.86 ksoftirqd/0
   5 root        0  -20    0    0    0 S    0   0.0   0:00.00 kworker/0:0H
   7 root      RT    0    0    0    0 S    0   0.0   0:01.44 migration/0
    
```

Related Commands

コマンド	説明
show platform software process slot switch	プラットフォーム ソフトウェア プロセスのスイッチ 情報を表示します。

show processes memory

各システムプロセスで使用されているメモリの量を表示するには、**show processes memory** コマンドを特権 EXEC モードで使用します。

show processes memory [*process-id* | **sorted** [**allocated** | **getbufs** | **holding**]]

Syntax Description

process-id	(任意) 特定のプロセスのプロセス ID (PID)。プロセス ID を指定すると、指定したプロセスの詳細のみが表示されます。
sorted	(任意) [Allocated]、[Get Buffers]、または [Holding] の列でソートされたメモリデータを表示します。 sorted キーワードを単独で使用した場合、データはデフォルトで [Holding] 列でソートされます。
allocated	(任意) [Allocated] 列でソートされたメモリデータを表示します。
getbufs	(任意) [Getbufs] (Get Buffers) 列でソートされたメモリデータを表示します。
holding	(任意) [Holding] 列でソートされたメモリデータを表示します。このキーワードがデフォルトです。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show processes memory コマンドと **show processes memory sorted** コマンドは、合計メモリ、使用済みメモリ、空きメモリの概要を表示し、その後にはプロセスとそれらがメモリに与える影響のリストを表示します。

標準の **show processes memory process-id** コマンドを使用すると、プロセスは PID でソートされます。**show processes memory sorted** コマンドを使用すると、デフォルトのソートは [Holding] によって行われます。



Note 特定のプロセスの保持メモリは、他のプロセスによっても割り当てられるため、割り当てられたメモリよりも大きくなる可能性があります。

次に、**show processes memory** コマンドの出力例を示します。

```
Device# show processes memory

Processor Pool Total: 25954228 Used: 8368640 Free: 17585588
PID TTY Allocated Freed Holding Getbufs Retbufs Process
0 0 8629528 689900 6751716 0 0 *Init*
```

show processes memory

```

0 0      24048      12928      24048          0          0 *Sched*
0 0          260          328           68      350080      0 *Dead*
1 0           0           0          12928          0          0 Chunk Manager
2 0          192          192          6928          0          0 Load Meter
3 0      214664          304      227288          0          0 Exec
4 0           0           0          12928          0          0 Check heaps
5 0           0           0          12928          0          0 Pool Manager
6 0          192          192          12928          0          0 Timers
7 0          192          192          12928          0          0 Serial Backgroun
8 0          192          192          12928          0          0 AAA high-capacit
9 0           0           0          24928          0          0 Policy Manager
10 0          0           0          12928          0          0 ARP Input
11 0          192          192          12928          0          0 DDR Timers
12 0           0           0          12928          0          0 Entity MIB API
13 0           0           0          12928          0          0 MPLS HC Counter
14 0           0           0          12928          0          0 SERIAL A'detect
.
.
.
78 0           0           0          12992          0          0 DHCPD Timer
79 0          160           0          13088          0          0 DHCPD Database
      8329440 Total

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 26: show processes memory のフィールドの説明

フィールド	説明
Processor Pool Total	プロセッサメモリプール用に保持されているメモリの合計量（キロバイト（KB）単位）。
Used	プロセッサメモリプール内の使用済みメモリの合計量（KB 単位）。
Free	プロセッサメモリプール内の空きメモリの合計量（KB 単位）。
PID	プロセス ID。
TTY	プロセスを制御する端末。
Allocated	プロセスによって割り当てられたメモリのバイト数。
Freed	最初に誰が割り当てたのかに関係なく、プロセスによって開放されたメモリのバイト数。
Holding	プロセスに現在割り当てられているメモリの量（KB 単位）。これには、プロセスによって割り当てられたメモリと、プロセスに割り当てられたメモリが含まれます。
Getbufs	プロセスがパケットバッファを要求した回数。
Retbufs	プロセスがパケットバッファを放棄した回数。
Process	プロセス名。
Init	システム初期化プロセス。

フィールド	説明
Sched	スケジューラプロセス。
Dead	現在は dead 状態にあるグループとしてのプロセス。
<value> Total	すべてのプロセスによって保持されているメモリの合計量 (KB 単位) ([Holding] 列の合計)。

次に、**sorted** キーワードを使用した場合の **show processes memory** コマンドの出力例を示します。この場合、出力は [Holding] 列で最大から最小へとソートされます。

Device# **show processes memory sorted**

```
Processor Pool Total: 25954228 Used: 8371280 Free: 17582948
PID TTY Allocated Freed Holding Getbufs Retbufs Process
  0  0 8629528 689900 6751716 0 0 *Init*
  3  0 217304 304 229928 0 0 Exec
 53  0 109248 192 96064 0 0 DHCPD Receive
 56  0 0 0 32928 0 0 COPS
 19  0 39048 0 25192 0 0 Net Background
 42  0 0 0 24960 0 0 L2X Data Daemon
 58  0 192 192 24928 0 0 X.25 Background
 43  0 192 192 24928 0 0 PPP IP Route
 49  0 0 0 24928 0 0 TCP Protocols
 48  0 0 0 24928 0 0 TCP Timer
 17  0 192 192 24928 0 0 XML Proxy Client
  9  0 0 0 24928 0 0 Policy Manager
 40  0 0 0 24928 0 0 L2X SSS manager
 29  0 0 0 24928 0 0 IP Input
 44  0 192 192 24928 0 0 PPP IPCP
 32  0 192 192 24928 0 0 PPP Hooks
 34  0 0 0 24928 0 0 SSS Manager
 41  0 192 192 24928 0 0 L2TP mgmt daemon
 16  0 192 192 24928 0 0 Dialer event
 35  0 0 0 24928 0 0 SSS Test Client
--More--
```

次に、プロセス ID (*process-id*) を指定したときの **show processes memory** コマンドの出力例を示します。

Device# **show processes memory 1**

```
Process ID: 1
Process Name: Chunk Manager
Total Memory Held: 8428 bytes
Processor memory holding = 8428 bytes
pc = 0x60790654, size = 6044, count = 1
pc = 0x607A5084, size = 1544, count = 1
pc = 0x6076DBC4, size = 652, count = 1
pc = 0x6076FF18, size = 188, count = 1
I/O memory holding = 0 bytes
```

Device# **show processes memory 2**

```
Process ID: 2
Process Name: Load Meter
Total Memory Held: 3884 bytes
Processor memory holding = 3884 bytes
pc = 0x60790654, size = 3044, count = 1
pc = 0x6076DBC4, size = 652, count = 1
```

show processes memory

```
pc = 0x6076FF18, size =      188, count =    1  
I/O memory holding = 0 bytes
```

Related Commands

Command	Description
show memory	空きメモリ プール統計情報を含む、メモリに関する統計情報を表示します。
show processes	アクティブなプロセスに関する情報を表示します。

show processes memory platform

各 Cisco IOS XE プロセスのメモリ使用率を表示するには、特権 EXEC モードで **show processes memory platform** コマンドを使用します。

```
show processes memory platform [ [ detailed { name process-name | process-id process-ID } [ location | maps [ location ] | smaps [ location ] ] | location | sorted [ location ] ] switch { switch-number | active | standby } { 0 | F0 | R0 } | accounting ]
```

Syntax Description	
accounting	(任意) 各 Cisco IOS XE プロセスの上位のメモリアロケータを表示します。
detailed	(任意) 指定された Cisco IOS XE プロセスの詳細なメモリ情報を表示します。
name process-name	(任意) Cisco IOS XE プロセス名を表示します。プロセス名を入力します。
process-id process-ID	(任意) Cisco IOS XE プロセス ID を表示します。プロセス ID を入力します。
location	(任意) Field Replaceable Unit (FRU) の場所に関する情報を表示します。
maps	(任意) プロセスのメモリ マップを表示します。
smaps	(任意) プロセスの静的メモリマップを表示します。
sorted	(任意) Cisco IOS XE プロセスによって使用されている常駐セットサイズ (RSS) メモリに基づいてソートされた出力を表示します。
switch switch-number	デバイスに関する情報を表示します。
active	デバイスのアクティブインスタンスに関する情報を表示します。
standby	デバイスのスタンバイインスタンスに関する情報を表示します。
0	共有ポートアダプタ (SPA) インターフェイス プロセッサ スロット 0 に関する情報を表示します。
F0	Embedded Service Processor (ESP) スロット 0 に関する情報を表示します。

show processes memory platform

R0 ルートプロセッサ（RP）スロット 0 に関する情報を表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが変更されました。キーワード accounting が追加されました。 出力から Total 列が削除されました。

Examples

次に、**show processes memory platform** コマンドの出力例を示します。

```
device# show processes memory platform

System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K
  Pid   Text      Data   Stack  Dynamic   RSS      Name
-----
    1   1246     4400   132    1308     4400      systemd
   96   233     2796   132     132     2796    systemd-journal
  105   284     1796   132     176     1796    systemd-udev
  707    52     2660   132     172     2660    in.telnetd
  744   968     3264   132    1700     3264    brelay.sh
  835    52     2660   132     172     2660    in.telnetd
  863   968     3264   132    1700     3264    brelay.sh
  928   968     3996   132    2312     3996    reflector.sh
  933   968     3976   132    2312     3976    droputil.sh
  934   968     2140   132     528     2140    oom.sh
  936   173     936    132     132     936     xinetd
  945   968     1472   132     132     1472    libvirtd.sh
  947   592    43164   132    3096    43164    repm
  954    45     932    132     132     932     rpcbind
  986   482    3476   132     132    3476    libvirtd
  988    66     940    132     132     940     rpc.statd
  993   968     928    132     132     928    boothelper_evt.
 1017   21     640    132     132     640    inotifywait
 1089  102    1200   132     132    1200    rpc.mountd
 1328    9    2940   132     148    2940    rotee
 1353   39     532    132     132     532     sleep
!
!
!
```

次に、**show processes memory platform accounting** コマンドの出力例を示します。

```
device# show processes memory platform accounting
Hourly Stats
```

process	callsite_ID(bytes)	max_diff_bytes	callsite_ID(calls)	
max_diff_calls	tracekey		timestamp (UTC)	
smand_rp_0	3624155137	172389	3624155138	50
1#a3e0e4361082c702e5bf1afbd90e6313		2018-09-04	14:23	
linux_iosd-imag_rp_0	3626295305	49188	3624155138	12
1#545420bd869d25eb5ab826182ee5d9ce		2018-09-04	12:03	
btman_rp_0	3624737792	17080	2953915394	64
1#d6888bd9564a3c4fcf049c31ba07a036		2018-09-04	22:29	
fman_fp_image_fp_0	3624059905	16960	4027402242	298
1#921ba4d9df5b0a6e946a3b270bd6592d		2018-09-04	22:55	
fed_main_event_fp_0	3626295305	16396	4027402242	32
1#27083f7bf3985d892505806cae2bfb0d		2018-09-04	12:03	
dbm_rp_0	3626295305	16396	4027402242	3
1#2b878f802bd7703c5298d37e7a4e8ac3		2018-09-04	12:02	
tamd_proc_rp_0	3895208962	12632	3624667171	7
1#5b0ed8f88ef5f873abcaf8a744037a44		2018-09-04	18:47	
btman_fp_0	3624233985	12288	3624737792	9
1#d6888bd9564a3c4fcf049c31ba07a036		2018-09-04	15:23	
sif_mgr_rp_0	3624059907	8216	4027402242	4
1#de2a951a8a7bae83ca2c04c56810eb72		2018-09-04	14:21	
python2.7_fp_0	2954560513	8000	2954560513	1
		2018-09-04	12:16	
nginx_rp_0	3357041665	4608	4027402242	4
1#32e56bb09e0509c5fa5ac32093631206		2018-09-04	16:18	
rotee_FRU_SLOT_NUM	3624667169	4097	3624667169	1
1#ff68e5150a698cd59fa259828614995b		2018-09-04	10:43	
hman_rp_0	3893617664	1488	3893617664	1
1#1c4aadada30083c5d6f66dc8ca8cd4cb		2018-09-04	10:42	
tams_proc_rp_0	3895096320	1024	3895096320	1
1#a36a3afa9884c8dc4d40af1e80cacc26		2018-09-04	10:42	
stack_mgr_rp_0	4027402242	904	4027402242	4
1#ca902eab11a18ab056b16554f49871e8		2018-09-04	14:21	
sessmgrd_rp_0	3491618816	848	3624155138	8
1#720239fc8bddcab059768c55a1640ed		2018-09-04	14:32	
psd_rp_0	4027402242	696	4027402242	4
1#98cf04e0ddd78c2400b3ca3b5f298594		2018-09-04	14:21	
lman_rp_0	4027402242	592	4027402242	4
1#dc8ed9e428d36477a617d56c51d5caf2		2018-09-04	14:21	
bt_logger_rp_0	4027402242	592	4027402242	4
1#ba882beled783e72575e97cc0908e0e8		2018-09-04	14:21	
repm_rp_0	4027402242	592	4027402242	4
1#ae461a05430efa767427f2ab40aba372		2018-09-04	14:21	
fman_rp_rp_0	4027402242	592	4027402242	3
1#09def9cc1390911be9e3a7a9c89f4cf7		2018-09-04	12:16	
epc_ws_liaison_fp_0	4027402242	592	4027402242	4
1#41451626dcce9d1478b22e2ebbbdcf54		2018-09-04	14:21	
cli_agent_rp_0	4027402242	592	4027402242	4
1#92d3882919daf3a9e210807c61de0552		2018-09-04	14:21	
cmm_rp_0	4027402242	592	4027402242	4
1#15ed1d79e96874b1e0621c42c3de6166		2018-09-04	14:21	
tms_rp_0	4027402242	352	4027402242	4
1#5c6efe2e21f15aa16318576d3ec9153c		2018-09-04	12:03	
plogd_rp_0	4027402242	48	4027402242	1
1#2d7f2ef57206f4fa763d7f2f5400bf1b		2018-09-04	10:43	
cmand_rp_0	3624155137	17	3624155137	1
1#f1f41f61c44d73014023db5d8a46ecf5		2018-09-04	10:42	
!				
!				
!				

次に、**show processes memory platform sorted** コマンドの出力例を示します。

```
device# show processes memory platform sorted
System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K
```

Pid	Text	Data	Stack	Dynamic	RSS	Name
7885	149848	684864	136	80	684864	linux_iosd-imag
9655	3787	264964	136	18004	264964	wcm
17261	324	248588	132	103908	248588	fed main event
4268	391	102084	136	5596	102084	cli_agent
4856	357	93388	132	3680	93388	dbm
17067	1087	77912	136	1796	77912	platform_mgr
!						
!						
!						

次に、**show processes memory platform sorted location switch active R0** コマンドの出力例を示します。

```
device# show processes memory platform sorted location switch active R0
System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K
```

Pid	Text	Data	Stack	Dynamic	RSS	Name
7885	149848	684864	136	80	684864	linux_iosd-imag
9655	3787	264964	136	18004	264964	wcm
17261	324	248588	132	103908	248588	fed main event
4268	391	102084	136	5596	102084	cli_agent
4856	357	93388	132	3680	93388	dbm
17067	1087	77912	136	1796	77912	platform_mgr
!						
!						
!						

show processes platform

プラットフォームで実行中の IOS-XE プロセスに関する情報を表示するには、特権 EXEC モードで **show processes platform** コマンドを使用します。

show processes platform [**detailed name** *process-name*] [**location** **switch** {*switch-number* | **active** | **standby**} {**0** | **F0** | **FP active** | **R0**}]

detailed	(任意) 指定した IOS-XE プロセスの詳細な情報を表示します。
name <i>process-name</i>	(任意) プロセス名を指定します。
location	(任意) Field Replaceable Unit (FRU) の場所を指定します。
switch <i>switch-number</i>	(任意) スイッチに関する情報を表示します。
active	(任意) デバイスのアクティブインスタンスを指定します。
standby	(任意) デバイスのスタンバイインスタンスを指定します。
0	共有ポートアダプタ (SPA) インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor (ESP) スロット 0 を指定します。
FP active	Embedded Service Processor (ESP) のアクティブインスタンスを指定します。
R0	ルート プロセッサ (RP) スロット 0 を指定します。

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Command Modes

特権 EXEC (#)

次に例を示します。

次に、**show processes platform** コマンドの出力例を示します。

```
Device# show processes platform

CPU utilization for five seconds: 1%, one minute: 2%, five minutes: 1%
  Pid   PPid  Status   Size  Name
-----
    1     0    S        4876  systemd
    2     0    S           0  kthreadd
    3     2    S           0  ksoftirqd/0
    5     2    S           0  kworker/0:0H
    7     2    S           0  rcu_sched
    8     2    S           0  rcu_bh
```

show processes platform

```

 9      2 S      0 migration/0
10      2 S      0 watchdog/0
11      2 S      0 watchdog/1
12      2 S      0 migration/1
13      2 S      0 ksoftirqd/1
15      2 S      0 kworker/1:0H
16      2 S      0 watchdog/2
17      2 S      0 migration/2
18      2 S      0 ksoftirqd/2
20      2 S      0 kworker/2:0H
21      2 S      0 watchdog/3
22      2 S      0 migration/3
23      2 S      0 ksoftirqd/3
24      2 S      0 kworker/3:0
25      2 S      0 kworker/3:0H
26      2 S      0 kdevtmpfs
27      2 S      0 netns
28      2 S      0 perf
29      2 S      0 khungtaskd
30      2 S      0 writeback
31      2 S      0 ksm
32      2 S      0 khugepaged
33      2 S      0 crypto
34      2 S      0 bioset
35      2 S      0 kblockd
36      2 S      0 ata_sff
37      2 S      0 rpciod
63      2 S      0 kswapd0
64      2 S      0 vmstat
65      2 S      0 fsnotify_mark
66      2 S      0 nfsiod
74      2 S      0 bioset
75      2 S      0 bioset
76      2 S      0 bioset
77      2 S      0 bioset
78      2 S      0 bioset
79      2 S      0 bioset
80      2 S      0 bioset
81      2 S      0 bioset
82      2 S      0 bioset
83      2 S      0 bioset
84      2 S      0 bioset
85      2 S      0 bioset
86      2 S      0 bioset
87      2 S      0 bioset
88      2 S      0 bioset
89      2 S      0 bioset
90      2 S      0 bioset
91      2 S      0 bioset
92      2 S      0 bioset
93      2 S      0 bioset
94      2 S      0 bioset
95      2 S      0 bioset
96      2 S      0 bioset
97      2 S      0 bioset
100     2 S      0 ipv6_addrconf
102     2 S      0 deferwq

```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 27: show processes platform のフィールドの説明

フィールド	説明
Pid	プロセス ID が表示されます。
PPid	親プロセスのプロセス ID が表示されます。
Status	人間が判読可能な形式でプロセスのステータスが表示されます。
Size	RAM でそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ（キロバイト（KB））が表示されます。
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。

show shell

シェルの情報を表示するには、ユーザ EXEC モードで **show shell** コマンドを使用します。

show shell [**enviornment** | **functions** [**brief** *shell_function*] | **triggers**]

Syntax Description	environment	(任意) シェル環境情報を表示します。
	functions [brief <i>shell_function</i>]	(任意) マクロ情報を表示します。 <ul style="list-style-type: none"> • brief: シェル関数の名前。 • <i>shell_function</i>: 1つのシェル関数の名
	triggers	(任意) イベント トリガー情報を表示し

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを使用して、スイッチのシェル情報を表示します。

例

次の例では、**show shell triggers** コマンドを使用して、スイッチソフトウェアに含まれているイベントトリガーを表示する方法を示します。

```
Device# term shell
Device# show shell triggers
User defined triggers
-----
Built-in triggers
-----
Trigger Id: CISCO_CUSTOM_EVENT
Trigger description: Custom macroevent to apply user defined configuration
Trigger environment: User can define the macro
Trigger mapping function: CISCO_CUSTOM_AUTOSMARTPORT

Trigger Id: CISCO_DMP_EVENT
Trigger description: Digital media-player device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
The value in the parenthesis is a default value
Trigger mapping function: CISCO_DMP_AUTO_SMARTPORT

Trigger Id: CISCO_IPVSC_EVENT
Trigger description: IP-camera device event to apply port configuration
```

```

Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
  The value in parenthesis is a default value
Trigger mapping function: CISCO_IP_CAMERA_AUTO_SMARTPORT

Trigger Id: CISCO_LAST_RESORT_EVENT
Trigger description: Last resortevent to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
  The value in the parenthesis is a default value
Trigger mapping function: CISCO_LAST_RESORT_SMARTPORT

Trigger Id: CISCO_PHONE_EVENT
Trigger description: IP-phone device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
and $VOICE_VLAN=(2), The value in the parenthesis is a default value
Trigger mapping function: CISCO_PHONE_AUTO_SMARTPORT

Trigger Id: CISCO_ROUTER_EVENT
Trigger description: Router device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1)
  The value in the parenthesis is a default value
Trigger mapping function: CISCO_ROUTER_AUTO_SMARTPORT

Trigger Id: CISCO_SWITCH_ETHERCHANNEL_CONFIG
Trigger description: etherchannel parameter
Trigger environment: $INTERFACE_LIST=(), $PORT-CHANNEL_ID=(),
                    $EC_MODE=(), $EC_PROTOCOLTYPE=(),
                    PORT-CHANNEL_TYPE=()
Trigger mapping function: CISCO_ETHERCHANNEL_AUTOSMARTPORT

Trigger Id: CISCO_SWITCH_EVENT
Trigger description: Switch device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1)
  The value in the parenthesis is a default value
Trigger mapping function: CISCO_SWITCH_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_AP_EVENT
Trigger description: Autonomous ap device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1)
  The value in the parenthesis is a default value
Trigger mapping function: CISCO_AP_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
Trigger description: Lightweight-ap device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
  The value in the parenthesis is a default value
Trigger mapping function: CISCO_LWAP_AUTO_SMARTPORT

Trigger Id: word
Trigger description: word
Trigger environment:
Trigger mapping function:

```

次の例では、**show shell functions** コマンドを使用して、スイッチソフトウェアに含まれている組み込みマクロを表示する方法を示します。

```

Device# show shell functions
#User defined functions:

#Built-in functions:
function CISCO_AP_AUTO_SMARTPORT () {
    if [[ $LINKUP == YES ]]; then
        conf t
            interface $INTERFACE

```

```

macro description $TRIGGER
switchport trunk encapsulation dot1q
switchport trunk native vlan $NATIVE_VLAN
switchport trunk allowed vlan ALL
switchport mode trunk
switchport nonegotiate
auto qos voip trust
mls qos trust cos
if [[ $LIMIT == 0 ]]; then
    default srr-queue bandwidth limit
else
    srr-queue bandwidth limit $LIMIT
fi
if [[ $SW_POE == YES ]]; then
    if [[ $AP125X == AP125X ]]; then
        macro description AP125X
        macro auto port sticky
        power inline port maximum 20000
    fi
fi
exit
end
fi
if [[ $LINKUP == NO ]]; then
    conf t
        interface $INTERFACE
            no macro description
            no switchport nonegotiate
            no switchport trunk native vlan $NATIVE_VLAN
            no switchport trunk allowed vlan ALL
            no auto qos voip trust
            no mls qos trust cos
            default srr-queue bandwidth limit
            if [[ $AUTH_ENABLED == NO ]]; then
                no switchport mode
                no switchport trunk encapsulation
            fi
            if [[ $STICKY == YES ]]; then
                if [[ $SW_POE == YES ]]; then
                    if [[ $AP125X == AP125X ]]; then
                        no macro auto port sticky
                        no power inline port maximum
                    fi
                fi
            fi
        fi
    exit
end
fi
}
<output truncated>

```

show system mtu

グローバル最大伝送ユニット（MTU）、またはスイッチに設定されている最大パケットサイズを表示するには、特権 EXEC モードで **show system mtu** コマンドを使用します。

```
show system mtu
```

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

なし

Command Modes

特権 EXEC（#）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

MTU 値および MTU 値に影響を与えるスタック設定の詳細については、**system mtu** コマンドを参照してください。

Examples

次に、**show system mtu** コマンドの出力例を示します。

```
Device# show system mtu
Global Ethernet MTU is 1500 bytes.
```

show tech-support

システム情報を表示する **show** コマンドを自動的に実行するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support

[**cef** | **cft** | **eigrp** | **evc** | **fnf** | **ipc** | **ipmulticast** | **ipsec** | **mfib** | **nat** | **nbar** | **onep** | **ospf** | **page** | **password** | **rsvp** | **subscriber** | **vrrp** | **wccp**]

Syntax Description

cef	(任意) CEF 関連情報を表示します。
cft	(任意) CFT 関連情報を表示します。
eigrp	(任意) EIGRP 関連情報を表示します。
evc	(任意) EVC 関連情報を表示します。
fnf	(任意) Flexible NetFlow 関連情報を表示します。
ipc	(任意) IPC 関連情報を表示します。
ipmulticast	(任意) IP 関連情報を表示します。
ipsec	(任意) IPSEC 関連情報を表示します。
isis	(任意) CLNS および ISIS 関連情報を表示します。
license	(任意) ライセンス関連情報を表示します。
lisp	(任意) Locator/ID Separation Protocol 関連情報を表示します。
メモリ	(任意) メモリ関連情報を表示します。
mfib	(任意) MFIB 関連情報を表示します。
msrp	(任意) MSRP 関連情報を表示します。
mvrp	(任意) MVRP 関連情報を表示します。
nat	(任意) NAT 関連情報を表示します。
onep	(任意) ONEP 関連情報を表示します。
ospf	(任意) OSPF 関連情報を表示します。
page	(任意) コマンド出力を 1 ページずつ表示します。Return キーを押して、出力の次の行を表示するか、スペースバーを使用して、次の情報ページを表示します。使用しない場合、出力がスクロールします (つまり、改ページで停止しません)。 コマンド出力を停止するには、 Ctrl+C キーを押します。

password	(任意) パスワードおよびその他のセキュリティ情報を出力に残します。使用しない場合、出力中のパスワードおよびその他のセキュリティ関連情報は、ラベル「<removed>」と置き換えられます。
performance-monitor	(任意) パフォーマンスモニタ関連情報を表示します。
pki	(任意) PKI 関連情報を表示します。
platform	(任意) プラットフォーム関連情報を表示します。
qos	(任意) QoS 関連情報を表示します。
subscriber	(任意) サブスクライバ関連情報を表示します。
switch-report	(任意) スイッチレポートをアーカイブします。
vrrp	(任意) VRRP 関連情報を表示します。
wccp	(任意) WCCP 関連情報を表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが実装されました。

Usage Guidelines

show tech-support コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします (たとえば、**show tech-support > filename**)。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。

リダイレクトには、次のいずれかの方法を使用できます。

- **> filename:** 出力をファイルにリダイレクトします。
- **>> filename:** 出力をファイルにアペンドモードでリダイレクトします。

show tech-support bgp

BGP 関連のシステム情報を表示する show コマンドを自動的に実行するには、特権 EXEC モードで **show tech-support bgp** コマンドを使用します。

```
show tech-support bgp [address-family {all | ipv4 [flowspec | multicast | unicast | [mdt | mvpn] {all | vrf vrf-instance-name} ] | ipv6 [flowspec | multicast | mvpn {all | vrf vrf-instance-name} | unicast] | l2vpn [evpn | vpls] | link-state [link-state] | [nsap | rtfiler] [unicast] | [vpn4 | vpn6] [flowspec | multicast | unicast] {all | vrf vrf-instance-name} } ] [detail]
```

Syntax Description	address-family	(任意) 指定したアドレスファミリの出力を表示します。
	address-family all	(任意) すべてのアドレスファミリの出力を表示します。
	ipv4	(任意) IPv4 アドレスファミリの出力を表示します。
	ipv6	(任意) IPv6 アドレスファミリの出力を表示します。
	l2vpn	(任意) L2VPN アドレスファミリの出力を表示します。
	link-state	(任意) リンク ステート アドレスファミリの出力を表示します。
	nsap	(任意) NSAP アドレスファミリの出力を表示します。
	rtfilter	(任意) RT フィルタ アドレスファミリの出力を表示します。
	vpn4	(任意) VPNv4 アドレスファミリの出力を表示します。
	vpn6	(任意) VPNv6 アドレスファミリの出力を表示します。
	flowspec	(任意) アドレスファミリのフロースペック関連情報を表示します。
	multicast	(任意) アドレスファミリのマルチキャスト関連情報を表示します。

unicast	(任意) アドレスファミリのユニキャスト関連情報を表示します。
mdt	(任意) アドレスファミリのマルチキャスト配信ツリー (MDT) 関連情報を表示します。
mvpn	(任意) アドレスファミリのマルチキャスト VPN (MVPN) 関連情報を表示します。
vrf	VPN ルーティング/転送インスタンスの情報を表示します。
evpn	(任意) アドレスファミリのイーサネット VPN (EVPN) 関連情報を表示します。
vpls	(任意) アドレスファミリの仮想プライベート LAN サービス (VPLS) 関連情報を表示します。
<i>vrf-instance-name</i>	VPN ルーティング/転送インスタンスの名前を指定します。
all	すべての VPN NLRI に関する情報を表示します。
detail	(任意) 詳細なルート情報を表示します。

Command Modes	ユーザ EXEC (>) 特権 EXEC (#)
----------------------	-----------------------------

Command History	リリース	変更内容
		このコマンドが導入されました。

Usage Guidelines **show tech-support bgp** コマンドは、さまざまな BGP show コマンドの出力を表示し、それらを show-tech ファイルに記録するために使用します。 **show tech-support bgp** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします (たとえば、**show tech-support > filename**)。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。

リダイレクトには、次のいずれかの方法を使用できます。

- > filename: 出力をファイルにリダイレクトします。
- >> filename: 出力をファイルにアペンドモードでリダイレクトします。

show tech-support bgp コマンドを使用すると、次の **show** コマンドが自動的に実行されます。

- **show clock**
- **show version**
- **show running-config**
- **show process cpu sorted**
- **show process cpu history**
- **show process memory sorted**

show tech-support bgp address-family*address-family-name address-family-modifier* コマンドを使用すると、特定のアドレスファミリに対する次の **show** コマンドが自動的に実行されます。

- **show bgp** *address-family-name address-family-modifier* **summary**
- **show bgp** *address-family-name address-family-modifier* **detail**
- **show bgp** *address-family-name address-family-modifier* **internal**
- **show bgp** *address-family-name address-family-modifier* **neighbors**
- **show bgp** *address-family-name address-family-modifier* **update-group**
- **show bgp** *address-family-name address-family-modifier* **replication**
- **show bgp** *address-family-name address-family-modifier* **community**
- **show bgp** *address-family-name address-family-modifier* **dampening dampened-paths**
- **show bgp** *address-family-name address-family-modifier* **dampening flap-statistics**
- **show bgp** *address-family-name address-family-modifier* **dampening parameters**
- **show bgp** *address-family-name address-family-modifier* **injected-paths**
- **show bgp** *address-family-name address-family-modifier* **cluster-ids**
- **show bgp** *address-family-name address-family-modifier* **cluster-ids internal**
- **show bgp** *address-family-name address-family-modifier* **peer-group**
- **show bgp** *address-family-name address-family-modifier* **pending-prefixes**
- **show bgp** *address-family-name address-family-modifier* **rib-failure**

show tech-support bgp コマンドを使用した場合は、上記のコマンドに加えて、セグメントルーティング固有の次の **show** コマンドも実行されます。

- **show bgp all binding-sid**
- **show segment-routing client**
- **show segment-routing mpls state**
- **show segment-routing mpls gb**
- **show segment-routing mpls connected-prefix-sid-map protocol ipv4**
- **show segment-routing mpls connected-prefix-sid-map protocol backup ipv4**

- **show mpls traffic-eng tunnel auto-tunnel client bgp**

show tech-support diagnostic

テクニカルサポートに使用する診断情報を表示するには、特権 EXEC モードで **show tech-support diagnostic** コマンドを使用します。

show tech-support diagnostic

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Usage Guidelines

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support diagnostic > flash:filename**）。



Note スタック構成をサポートしているデバイスの場合、このコマンドはアップしているすべてのスイッチで実行されます。スタック構成をサポートしていないデバイスの場合、このコマンドはアクティブスイッチでのみ実行されます。

このコマンドの出力には次のコマンドの出力が表示されます。

- **show clock**
- **show version**
- **show running-config**
- **show inventory**
- **show diagnostic bootup level**
- **show diagnostic status**
- **show diagnostic content switch all**
- **show diagnostic result switch all detail**
- **show diagnostic schedule switch all**
- **show diagnostic post**
- **show diagnostic description switch [switch number] test all**
- **show logging onboard switch [switch number] clilog detail**
- **show logging onboard switch [switch number] counter detail**

- **show logging onboard switch [switch number] environment detail**
- **show logging onboard switch [switch number] message detail**
- **show logging onboard switch [switch number] poe detail**
- **show logging onboard switch [switch number] status**
- **show logging onboard switch [switch number] temperature detail**
- **show logging onboard switch [switch number] uptime detail**
- **show logging onboard switch [switch number] voltage detail**

speed

ポートの速度を指定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。



Note 使用可能な設定オプションは、スイッチモデルおよび取り付けられているトランシーバモジュールによって異なります。オプションには、10、100、1000、2500、5000、10000、25000、40000、100000 があります。

```
speed {10 | 100 | 1000 | 2500 | 5000 | auto [10 | 100 | 1000 | 2500 | 5000] | nonegotiate}
no speed
```

Syntax Description		
10	ポートが 10 Mbps で稼働することを指定します。	
100	ポートが 100 Mbps で稼働することを指定します。	
1000	ポートが 1000 Mbps で稼働することを指定します。このオプションは、10/100/1000 Mb/s ポートでだけ有効になって表示されます。	
2500	ポートが 2500 Mbps で稼働することを指定します。このオプションは、マルチギガビット対応のイーサネット ポートでのみ有効であり、表示されます。	
5000	ポートが 5000 Mbps で稼働することを指定します。このオプションは、マルチギガビット対応のイーサネット ポートでのみ有効であり、表示されます。	
auto	稼働時のポートの速度を、リンクのもう一方の終端のポートを基準にして自動的に検出します。 auto キーワードと一緒に 10 、 100 、 1000 、 2500 、または 5000 キーワードを使用した場合、ポートは指定の速度でのみ自動ネゴシエートします。	
nonegotiate	自動ネゴシエーションをディセーブルにし、ポートは 1000 Mbps で稼働します。	

Command Default デフォルトは **auto** です。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 10 ギガビット イーサネット ポートでは速度を設定できません。

1000BASE-T Small Form-Factor Pluggable (SFP) モジュールを除き、SFP モジュールポートが自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように (**nonegotiate**) 速度を設定できます。

キーワード **2500** および **5000** は、マルチギガビット (m-Gig) イーサネット対応デバイスでのみ表示されます。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にあるデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

ラインの両端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーション設定を使用することを強く推奨します。一方のインターフェイスでは自動ネゴシエーションをサポートし、もう一方の終端ではサポートしていない場合、サポートしている側には **auto** 設定を使用し、サポートしていない終端にはデュプレックスおよび速度を設定します。



Caution インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーションガイドの「[Configuring Interface Characteristics](#)」の章を参照してください。

設定を確認するには、**show interfaces** 特権 EXEC コマンドを使用します。

Examples

次に、ポートの速度を 100 Mbps に設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed 100
```

次に、10 Mbps でだけポートが自動ネゴシエートするように設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10
```

次に、10 Mbps または 100 Mbps でだけポートが自動ネゴシエートするように設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10 100
```

start (COAP プロキシ コンフィギュレーション)

スイッチで CoAP を開始するには、COAP プロキシ コンフィギュレーション モードで **start** コマンドを使用します。

start

Command Modes COAP プロキシ コンフィギュレーション (config-coap-proxy)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines COAP プロキシ コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで **coap proxy** コマンドを入力します。

例

次に、スイッチで CoAP を開始する例を示します。

```
Device(config)# coap proxy
Device(config-coap-proxy)# start
```

stop (COAP プロキシ コンフィギュレーション)

スイッチで CoAP を停止するには、COAP プロキシ コンフィギュレーション モードで **stop** コマンドを使用します。

stop

Command Modes COAP プロキシ コンフィギュレーション (config-coap-proxy)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines COAP プロキシ コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで **coap proxy** コマンドを入力します。

例

次に、スイッチで CoAP を停止する例を示します。

```
Device(config)# coap proxy  
Device(config-coap-proxy)# stop
```

switchport block

不明なマルチキャストまたはユニキャストパケットが転送されないようにするには、インターフェイス コンフィギュレーションモードで **switchport block** コマンドを使用します。不明なマルチキャストまたはユニキャストパケットの転送を許可するには、このコマンドの **no** 形式を使用します。

```
switchport block {multicast|unicast}
no switchport block {multicast|unicast}
```

Syntax Description

multicast 不明のマルチキャストトラフィックがブロックされるように指定します。

Note 純粋なレイヤ2 マルチキャストトラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャストパケットはブロックされません。

unicast 不明のユニキャストトラフィックがブロックされるように指定します。

Command Default

不明なマルチキャストおよびユニキャストトラフィックはブロックされていません。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デフォルトでは、不明な MAC アドレスを持つすべてのトラフィックがすべてのポートに送信されます。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャストトラフィックをブロックすることができます。不明なマルチキャストまたはユニキャストトラフィックが保護ポートでブロックされない場合、セキュリティに問題のある場合があります。

マルチキャストトラフィックでは、ポートブロッキング機能は純粋なレイヤ2パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャストパケットはブロックされません。

不明なマルチキャストまたはユニキャストトラフィックのブロックは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

パケットのブロックに関する情報は、このリリースに対応するソフトウェア コンフィギュレーションガイドを参照してください。

次の例では、インターフェイス上で不明なユニキャストトラフィックをブロックする方法を示します。

```
Device(config-if)# switchport block unicast
```

設定を確認するには、**show interfaces *interface-id* switchport** 特権 EXEC コマンドを入力します。

system mtu

ギガビットイーサネットおよび10ギガビットイーサネットポートのスイッチドパケットのグローバル最大パケットサイズまたはMTUサイズを設定するには、グローバル コンフィギュレーションモードで **system mtu** コマンドを使用します。グローバル MTU 値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system mtu bytes
no system mtu

Syntax Description	<i>bytes</i> グローバル MTU のサイズ（バイト単位）。指定できる範囲は、1500 ～ 9198 バイトです。デフォルトは 1500 バイトです。	
Command Default	すべてのポートのデフォルトの MTU サイズは 1500 バイトです。	
Command Modes	グローバル コンフィギュレーション（config）	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 設定を確認するには、**show system mtu** 特権 EXEC コマンドを入力します。

スイッチはインターフェイス単位では MTU をサポートしていません。

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。

Examples

次に、グローバル システム MTU サイズを 6000 バイトに設定する例を示します。

```
Device(config)# system mtu 6000
Global Ethernet MTU is set to 6000 bytes.
Note: this is the Ethernet payload size, not the total
Ethernet frame size, which includes the Ethernet
header/trailer and possibly other tags, such as ISL or
802.1q tags.
```

transport (COAP プロキシ コンフィギュレーション)

トランスポートプロトコルを設定するには、COAP プロキシ コンフィギュレーション モードで **transport** コマンドを使用します。

```
transport {tcp | udp}
```

Syntax Description	tcp	TCP プロトコルを指定します。
	udp	UDP プロトコルを指定します。
Command Modes	COAP プロキシ コンフィギュレーション (config-coap-proxy)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	COAP プロキシ コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで coap proxy コマンドを入力します。	

例

次に、TCP をトランスポートプロトコルとして設定する例を示します。

```
Device(config)# coap proxy
Device(config-coap-proxy)# transport tcp
```

voice-signaling vlan (ネットワークポリシー コンフィギュレーション)

音声シグナリング アプリケーション タイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice-signaling vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice-signaling vlan {*vlan-id* [**cos** *cos-value* | **dscp** *dscp-value*] | **dot1p** [**cos** *l2-priority* | **dscp** *dscp*] | **none** | **untagged**}

Syntax Description	
vlan-id	(任意) 音声トラフィック用の VLAN。指定できる範囲は 1 ~ 4094 です。
cos <i>cos-value</i>	(任意) 設定された VLAN に対する レイヤ 2 プライオリティ Class of Service (CoS) を指定します。指定できる範囲は 0 ~ 7 です。デフォルト値は 5 です。
dscp <i>dscp-value</i>	(任意) 設定された VLAN に対する Diffserv コード ポイント (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 です。デフォルト値は 46 です。
dot1p	(任意) IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように電話を設定します。
none	(任意) 音声 VLAN に関して Cisco IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	(任意) タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

Command Default	
	音声シグナリング アプリケーション タイプのネットワークポリシー プロファイルは定義されていません。
	デフォルトの CoS 値は、5 です。
	デフォルトの DSCP 値は、46 です。
	デフォルトのタギング モードは、untagged です。

Command Modes	ネットワークポリシー プロファイル コンフィギュレーション
---------------	-------------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードを開始するには、 network-policy profile グローバル コンフィギュレーション コマンドを使用します。
------------------	--

voice-signaling アプリケーションタイプは、音声メディアと異なる音声シグナリング用のポリシーを必要とするネットワーク トポロジ用です。すべての同じネットワーク ポリシーが voice policy TLV にアドバタイズされたポリシーとして適用される場合、このアプリケーションタイプはアドバタイズしないでください。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service (CoS)、Diffserv コード ポイント (DSCP) の値、およびタギング モードを指定することで、音声シグナリング用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) の network-policy Time Length Value (TLV) に含まれます。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

次の例では、プライオリティ 2 の CoS を持つ VLAN 200 用の音声シグナリングを設定する方法を示します。

```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice-signaling vlan 200 cos 2
```

次の例では、DSCP 値 45 を持つ VLAN 400 用の音声シグナリングを設定する方法を示します。

```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice-signaling vlan 400 dscp 45
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声シグナリングを設定する方法を示します。

```
デバイス(config-network-policy)# voice-signaling vlan dot1p cos 4
```

voice vlan (ネットワークポリシー コンフィギュレーション)

音声アプリケーションタイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

```
voice vlan {vlan-id [cos cos-value | dscp dscp-value] | dot1p [cos l2-priority | dscp dscp] | none | untagged}
```

Syntax Description	
vlan-id	(任意) 音声トラフィック用の VLAN。指定できる範囲は 1 ~ 4094 です。
cos <i>cos-value</i>	(任意) 設定された VLAN に対するレイヤ 2 プライオリティ Class of Service (CoS) を指定します。指定できる範囲は 0 ~ 7 です。デフォルト値は 5 です。
dscp <i>dscp-value</i>	(任意) 設定された VLAN に対する Diffserv コードポイント (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 です。デフォルト値は 46 です。
dot1p	(任意) IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように電話を設定します。
none	(任意) 音声 VLAN に関して Cisco IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	(任意) タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

Command Default 音声アプリケーションタイプのネットワークポリシー プロファイルは定義されていません。
デフォルトの CoS 値は、5 です。
デフォルトの DSCP 値は、46 です。
デフォルトのタギング モードは、untagged です。

Command Modes ネットワークポリシー プロファイル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードを開始するには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。

voice アプリケーション タイプは IP Phone 専用であり、対話形式の音声サービスをサポートするデバイスに似ています。通常、これらのデバイスは、展開を容易に行えるようにし、データアプリケーションから隔離してセキュリティを強化するために、別個の VLAN に配置されます。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service (CoS)、Diffserv コードポイント (DSCP) の値、およびタギング モードを指定することで、音声用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) の network-policy Time Length Value (TLV) に含まれます。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

次の例では、プライオリティ 4 の CoS を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice vlan 100 cos 4
```

次の例では、DSCP 値 34 を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice vlan 100 dscp 34
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
デバイス(config-network-policy)# voice vlan dot1p cos 4
```




PART **IV**

IP アドレッシングサービス

- [IP アドレッシング サービス コマンド, on page 415](#)



IP アドレッシング サービス コマンド

- [clear ipv6 access-list](#), on page 419
- [clear ipv6 dhcp](#), on page 420
- [clear ipv6 dhcp binding](#), on page 421
- [clear ipv6 dhcp client](#), on page 423
- [clear ipv6 dhcp conflict](#), on page 424
- [clear ipv6 dhcp relay binding](#), on page 425
- [clear ipv6 eigrp](#), on page 426
- [clear ipv6 mfib counters](#), on page 427
- [clear ipv6 mld counters](#), on page 428
- [clear ipv6 mld traffic](#), on page 429
- [clear ipv6 mtu](#), on page 430
- [clear ipv6 multicast aaa authorization](#), on page 431
- [clear ipv6 nd destination](#), on page 432
- [clear ipv6 nd on-link prefix](#), on page 433
- [clear ipv6 nd router](#), on page 434
- [clear ipv6 neighbors](#), on page 435
- [clear ipv6 ospf](#), on page 437
- [clear ipv6 ospf counters](#), on page 438
- [clear ipv6 ospf events](#), on page 440
- [clear ipv6 pim reset](#), on page 441
- [clear ipv6 pim topology](#), on page 442
- [clear ipv6 pim traffic](#), on page 443
- [clear ipv6 prefix-list](#), on page 444
- [clear ipv6 rip](#), on page 446
- [clear ipv6 route](#), on page 448
- [clear ipv6 spd](#), on page 449
- [fhrp delay](#), on page 450
- [fhrp version vrrp v3](#), on page 451
- [ip address dhcp](#), on page 452
- [ip address pool \(DHCP\)](#), on page 456
- [ip address](#), on page 457
- [ip unnumbered](#), on page 460
- [ip wccp](#), on page 462

- ipv6 access-list, on page 468
- ipv6 address-validate, on page 472
- ipv6 cef, on page 473
- ipv6 cef accounting, on page 475
- ipv6 cef distributed, on page 478
- ipv6 cef load-sharing algorithm, on page 480
- ipv6 cef optimize neighbor resolution, on page 482
- ipv6 destination-guard policy, on page 483
- ipv6 dhcp-relay bulk-lease, on page 484
- ipv6 dhcp-relay option vpn, on page 485
- ipv6 dhcp-relay source-interface, on page 486
- ipv6 dhcp binding track ppp, on page 487
- ipv6 dhcp database, on page 489
- ipv6 dhcp iana-route-add, on page 491
- ipv6 dhcp iapd-route-add, on page 492
- **ipv6 dhcp-ldra** , on page 493
- ipv6 dhcp ping packets, on page 494
- ipv6 dhcp pool, on page 495
- ipv6 dhcp server vrf enable, on page 498
- ipv6 flow monitor , on page 499
- ipv6 general-prefix, on page 500
- ipv6 local policy route-map, on page 502
- ipv6 local pool, on page 504
- ipv6 mld snooping (グローバル) , on page 506
- ipv6 mld ssm-map enable, on page 507
- ipv6 mld state-limit, on page 508
- ipv6 multicast-routing, on page 510
- ipv6 multicast group-range, on page 511
- ipv6 multicast pim-passive-enable, on page 513
- ipv6 nd cache expire, on page 514
- ipv6 nd cache interface-limit (global), on page 516
- ipv6 nd host mode strict, on page 517
- ipv6 nd na glean, on page 518
- ipv6 nd ns-interval, on page 519
- ipv6 nd nud retry, on page 520
- ipv6 nd reachable-time, on page 522
- ipv6 nd resolution data limit, on page 523
- ipv6 nd route-owner, on page 524
- ipv6 neighbor, on page 525
- ipv6 ospf name-lookup, on page 527
- ipv6 pim, on page 528
- ipv6 pim accept-register, on page 529
- ipv6 pim allow-rp , on page 530
- ipv6 pim neighbor-filter list, on page 531
- ipv6 pim rp-address, on page 532
- ipv6 pim rp embedded, on page 535

- ipv6 pim spt-threshold infinity, on page 536
- ipv6 prefix-list, on page 537
- ipv6 source-guard attach-policy, on page 540
- ipv6 source-route, on page 541
- ipv6 spd mode, on page 543
- ipv6 spd queue max-threshold, on page 545
- ipv6 traffic interface-statistics, on page 546
- ipv6 unicast-routing, on page 547
- key chain, on page 548
- key-string (認証) , on page 549
- key, on page 550
- show ip ports all, on page 552
- show ipv6 access-list, on page 554
- show ipv6 destination-guard policy, on page 557
- show ipv6 dhcp, on page 558
- show ipv6 dhcp binding, on page 559
- show ipv6 dhcp conflict, on page 562
- show ipv6 dhcp database, on page 563
- show ipv6 dhcp guard policy, on page 565
- show ipv6 dhcp interface, on page 567
- show ipv6 dhcp relay binding, on page 570
- show ipv6 eigrp events, on page 572
- show ipv6 eigrp interfaces, on page 574
- show ipv6 eigrp topology, on page 577
- show ipv6 eigrp traffic, on page 579
- show ipv6 general-prefix, on page 581
- show ipv6 interface, on page 583
- show ipv6 mfib, on page 592
- show ipv6 mld groups, on page 598
- show ipv6 mld interface, on page 601
- show ipv6 mld snooping, on page 604
- show ipv6 mld ssm-map, on page 606
- show ipv6 mld traffic, on page 608
- show ipv6 mrrib client, on page 610
- show ipv6 mrrib route, on page 612
- show ipv6 mroute, on page 615
- show ipv6 mtu, on page 620
- show ipv6 nd destination, on page 622
- show ipv6 nd on-link prefix, on page 624
- show ipv6 neighbors, on page 625
- show ipv6 ospf, on page 630
- show ipv6 ospf border-routers, on page 634
- show ipv6 ospf event, on page 636
- show ipv6 ospf graceful-restart, on page 639
- show ipv6 ospf interface, on page 641
- show ipv6 ospf request-list, on page 646

- [show ipv6 ospf retransmission-list](#), on page 648
- [show ipv6 ospf statistics](#), on page 650
- [show ipv6 ospf summary-prefix](#), on page 652
- [show ipv6 ospf timers rate-limit](#), on page 653
- [show ipv6 ospf traffic](#), on page 654
- [show ipv6 ospf virtual-links](#), on page 658
- [show ipv6 pim anycast-RP](#), on page 660
- [show ipv6 pim bsr](#), on page 661
- [show ipv6 pim df](#), on page 664
- [show ipv6 pim group-map](#), on page 666
- [show ipv6 pim interface](#), on page 668
- [show ipv6 pim join-prune statistic](#), on page 670
- [show ipv6 pim limit](#), on page 672
- [show ipv6 pim neighbor](#), on page 673
- [show ipv6 pim range-list](#), on page 675
- [show ipv6 pim topology](#), on page 677
- [show ipv6 pim traffic](#), on page 680
- [show ipv6 pim tunnel](#), on page 682
- [show ipv6 policy](#), on page 684
- [show ipv6 prefix-list](#), on page 685
- [show ipv6 protocols](#), on page 688
- [show ipv6 rip](#), on page 690
- [show ipv6 routers](#), on page 696
- [show ipv6 rpf](#), on page 699
- [show ipv6 source-guard policy](#), on page 701
- [show ipv6 spd](#), on page 702
- [show ipv6 static](#), on page 703
- [show ipv6 traffic](#), on page 707
- [show key chain](#), on page 710
- [show track](#), on page 711
- [track](#), on page 713
- [vrrp](#), on page 715
- [vrrp description](#), on page 716
- [vrrp preempt](#), on page 717
- [vrrp priority](#), on page 719
- [vrrp timers advertise](#), on page 720
- [vrrs leader](#), on page 722

clear ipv6 access-list

IPv6 アクセスリストの一致カウンタをリセットするには、特権 EXEC モードで **clear ipv6 access-list** コマンドを使用します。

clear ipv6 access-list [*access-list-name*]

Syntax Description

<i>access-list-name</i>	(任意) 一致カウンタをクリアする IPv6 アクセスリストの名前。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
-------------------------	--

Command Default

リセットは開始されません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear ipv6 access-list コマンドは、IPv6 固有である点を除いて、**clear ip access-list counters** コマンドに似ています。

access-list-name 引数なしで **clear ipv6 access-list** コマンドを使用すると、ルータに設定されているすべての IPv6 アクセスリストの一致カウンタがリセットされます。

このコマンドは、IPv6 グローバル ACL ハードウェアカウンタをリセットします。

Examples

次に、marketing という IPv6 アクセスリストの一致カウンタをリセットする例を示します。

```
デバイス# clear ipv6 access-list marketing
```

Related Commands

コマンド	説明
hardware statistics	ハードウェア統計情報の収集をイネーブルにします。
ipv6 access-list	IPv6 アクセスリストを定義し、IPv6 アクセスリストコンフィギュレーションモードを開始します。
show ipv6 access-list	現在のすべての IPv6 アクセスリストの内容を表示します。

clear ipv6 dhcp

IPv6 Dynamic Host Configuration Protocol (DHCP) 情報をクリアするには、特権 EXEC モードで **clear ipv6 dhcp** コマンドを使用します。

clear ipv6 dhcp

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **clear ipv6 dhcp** コマンドは IPv6 の DHCP 情報を削除します。

Examples 次に例を示します。

```
デバイス# clear ipv6 dhcp
```

clear ipv6 dhcp binding

IPv6 サーバのバインディングテーブルの Dynamic Host Configuration Protocol (DHCP) から自動クライアントバインディングを削除するには、特権 EXEC モードで **clear ipv6 dhcp binding** コマンドを使用します。

clear ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description	
<i>ipv6-address</i>	(任意) IPv6 クライアントの DHCP のアドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **clear ipv6 dhcp binding** コマンドはサーバ関数として使用します。

IPv6 用 DHCP サーバのバインディング テーブル エントリに対して、次の処理が自動的に行われます。

- コンフィギュレーション プールからプレフィックスがクライアントに委任されるたびに作成されます。
- クライアントがプレフィックスの委任を更新、再バインディング、または確認すると更新されます。
- クライアントがバインディング内のすべてのプレフィックスを自発的に解放したか、すべてのプレフィックスの有効期限が切れたか、または管理者が **clear ipv6 dhcp binding** コマンドを実行した場合に、削除されます。

clear ipv6 dhcp binding コマンドをオプションの *ipv6-address* 引数とともに使用すると、特定のクライアントのバインディングのみが削除されます。**clear ipv6 dhcp binding** コマンドを *ipv6-address* 引数なしで使用すると、IPv6 バインディングテーブルの DHCP からすべての自動クライアントバインディングが削除されます。オプションの **vrf** *vrf-name* キーワードと引数の組み合わせを使用すると、特定の VRF のバインディングのみがクリアされます。

Examples

次に、IPv6 サーバのバインディングテーブルの DHCP からすべての自動クライアントバインディングを削除する例を示します。

clear ipv6 dhcp binding

デバイス# `clear ipv6 dhcp binding`

Related Commands

Command	Description
<code>show ipv6 dhcp binding</code>	IPv6 サーバのバインディングテーブルの DHCP から自動クライアントバインディングを表示します。

clear ipv6 dhcp client

インターフェイス上の IPv6 クライアントの Dynamic Host Configuration Protocol (DHCP) を再起動するには、特権 EXEC モードで **clear ipv6 dhcp client** コマンドを使用します。

clear ipv6 dhcp client *interface-type interface-number*

Syntax Description	<i>interface-type interface-number</i>	インターフェイスのタイプと番号。詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
---------------------------	--	---

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **clear ipv6 dhcp client** コマンドは、以前に取得したプレフィックスとその他のコンフィギュレーションオプション (ドメインネームシステム (DNS) サーバなど) を最初に解放し、設定を解除した後に、特定のインターフェイス上の IPv6 クライアントの DHCP を再起動します。

Examples

次に、イーサネット インターフェイス 1/0 の IPv6 クライアントの DHCP を再起動する例を示します。

```
デバイス# clear ipv6 dhcp client Ethernet 1/0
```

Related Commands	Command	Description
	show ipv6 dhcp interface	IPv6 用 DHCP のインターフェイス情報を表示します。

clear ipv6 dhcp conflict

IPv6 (DHCPv6) サーバデータベースの Dynamic Host Configuration Protocol からアドレス競合をクリアするには、特権 EXEC モードで **clear ipv6 dhcp conflict** コマンドを使用します。

```
clear ipv6 dhcp conflict {*ipv6-address | vrf vrf-name }
```

Syntax Description

*	すべてのアドレス競合をクリアします。
ipv6-address	競合するアドレスを含むホスト IPv6 アドレスをクリアします。
vrf vrf-name	Virtual Routing and Forwarding (VRF) 名を指定します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。クライアントはネイバー探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

アドレスパラメータとしてアスタリスク (*) 文字を使用すると、DHCP はすべての競合をクリアします。

vrf vrf-name キーワードと引数を指定すると、特定の VRF に属しているアドレス競合のみがクリアされます。

Examples

次に、DHCPv6 サーバデータベースからすべてのアドレス競合をクリアする例を示します。

```
デバイス# clear ipv6 dhcp conflict *
```

Related Commands

コマンド	説明
show ipv6 dhcp conflict	アドレスをクライアントに提供する際に DHCPv6 サーバによって検出されたアドレス競合を表示します。

clear ipv6 dhcp relay binding

IPv6 リレーバインディングの Dynamic Host Configuration Protocol (DHCP) の IPv6 アドレスまたは IPv6 プレフィックスをクリアするには、特権 EXEC モードで **clear ipv6 dhcp relay binding** コマンドを使用します。

```
clear ipv6 dhcp relay binding {vrf vrf-name} {*ipv6-addressipv6-prefix}
```

```
clear ipv6 dhcp relay binding {vrf vrf-name} {*ipv6-prefix}
```

Syntax Description	Parameter	Description
	vrf vrf-name	Virtual Routing and Forwarding (VRF) のコンフィギュレーションを指定します。
	*	すべての DHCPv6 リレーバインディングをクリアします。
	<i>ipv6-address</i>	DHCPv6 アドレス。
	<i>ipv6-prefix</i>	IPv6 prefix.

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **clear ipv6 dhcp relay binding** コマンドは、IPv6 リレーバインディングの DHCP の特定の IPv6 アドレスまたは IPv6 プレフィックスを削除します。リレークライアントを指定しないと、バインディングは削除されません。

Examples

次に、指定した IPv6 アドレスを持つクライアントのバインディングをクリアする例を示します。

```
デバイス# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

次に、Cisco uBR10012 ユニバーサルブロードバンドデバイス上の vrf1 という VRF 名と特定のプレフィックスを持つクライアントのバインディングをクリアする例を示します。

```
デバイス# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8:0:1::/64
```

Related Commands	コマンド	説明
	show ipv6 dhcp relay binding	リレーエージェント上の DHCPv6 IANA バインディングと DHCPv6 IAPD バインディングを表示します。

clear ipv6 eigrp

IPv6 ルーティングテーブルの Enhanced Interior Gateway Routing Protocol (EIGRP) からエントリを削除するには、特権 EXEC モードで **clear ipv6 eigrp** コマンドを使用します。

clear ipv6 eigrp [*as-number*] [**neighbor** [*ipv6-address* | *interface-type interface-number*]]

Syntax Description

<i>as-number</i>	(任意) 自律システム番号。
neighbor	(任意) ネイバルータのエントリを削除します。
<i>ipv6-address</i>	(任意) 隣接ルータの IPv6 アドレス。
<i>interface-type</i>	(任意) ネイバルータのインターフェイスタイプ。
<i>interface-number</i>	(任意) ネイバルータのインターフェイス番号。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IPv6 ルーティングテーブルエントリのすべての EIGRP をクリアするには、引数およびキーワードを指定せずに **clear ipv6 eigrp** コマンドを使用します。指定したプロセスのルーティングテーブルのエントリをクリアするには *as-number* 引数を使用し、ネイバートーブルから特定のネイバーを削除するには **neighbor***ipv6-address* キーワードと引数、または *interface-typeinterface-number* 引数を使用します。

Examples

次に、IPv6 アドレスが 3FEE:12E1:2AC1:EA32 のネイバーを削除する例を示します。

```
デバイス# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32
```

clear ipv6 mfib counters

アクティブなすべてのマルチキャスト転送情報ベース（MFIB）のトラフィックカウンタをリセットするには、特権 EXEC モードで **clear ipv6 mfib counters** コマンドを使用します。

clear ipv6 mfib [**vrf** *vrf-name*] **counters** [*group-name* | *group-address* [*source-address* *source-name*]]

Syntax Description		
vrf <i>vrf-name</i>		（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
<i>group-name</i> <i>group-address</i>		（任意）マルチキャストグループの IPv6 アドレスまたは名前。
<i>source-address</i> <i>source-name</i>		（任意）送信元の IPv6 アドレスまたは名前。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **clear ipv6 mfib counters** コマンドを有効にした後、トラフィックカウンタを表示する次の show コマンドのいずれかを使用して追加のトラフィックを転送するかどうかを決定できます。

- **show ipv6 mfib**
- **show ipv6 mfib active**
- **show ipv6 mfib count**
- **show ipv6 mfib interface**
- **show ipv6 mfib summary**

Examples

次に、すべての MFIB トラフィックカウンタをクリアしてからリセットする例を示します。

```
デバイス# clear ipv6 mfib counters
```

clear ipv6 mld counters

マルチキャストリスナー検出（MLD）インターフェイスカウンタをクリアするには、特権 EXEC モードで **clear ipv6 mld counters** コマンドを使用します。

clear ipv6 mld [**vrf vrf-name**] **counters** [*interface-type*]

Syntax Description

<i>vrf vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
<i>interface-type</i>	（任意）インターフェイスタイプ。詳細については、疑問符（?）を使用してオンラインヘルプを参照してください。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

受信した参加および脱退の数を追跡する MLD カウンタをクリアするには、**clear ipv6 mld counters** コマンドを使用します。オプションの *interface-type* 引数を省略した場合、**clear ipv6 mld counters** コマンドはすべてのインターフェイスのカウンタをクリアします。

Examples

次に、イーサネット インターフェイス 1/0 のカウンタをクリアする例を示します。

```
デバイス# clear ipv6 mld counters Ethernet1/0
```

Related Commands

コマンド	説明
show ipv6 mld interface	インターフェイスのマルチキャスト関連情報を表示します。

clear ipv6 mld traffic

マルチキャストリスナー検出 (MLD) トラフィックカウンタをリセットするには、特権 EXEC モードで **clear ipv6 mld traffic** コマンドを使用します。

clear ipv6 mld [*vrf vrf-name*] **traffic**

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
----------------------------	--

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear ipv6 mld traffic コマンドを使用して、すべての MLD トラフィックカウンタをリセットします。

Examples

次に、MLD トラフィックカウンタをリセットする例を示します。

```
デバイス# clear ipv6 mld traffic
```

コマンド	説明
show ipv6 mld traffic	MLD トラフィックカウンタを表示します。

clear ipv6 mtu

メッセージの最大伝送ユニット（MTU）のキャッシュをクリアするには、特権 EXEC モードで **clear ipv6 mtu** コマンドを使用します。

clear ipv6 mtu

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default メッセージは、MTU キャッシュからはクリアされません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ルータが ICMPv6 toobig メッセージでフラッドしている場合、そのルータは利用可能なすべてのメモリが消費されるまで、MTU キャッシュ内にエントリを無制限に作成します。MTU キャッシュからメッセージをクリアするには、**clear ipv6 mtu** コマンドを使用します。

Examples 次に、メッセージの MTU をクリアする例を示します。

```
デバイス# clear ipv6 mtu
```

Related Commands	コマンド	説明
	ipv6 flowset	ルータによって送信された 1,280 バイト以上のパケット内にフローラベルマーキングを設定します。

clear ipv6 multicast aaa authorization

IPv6 マルチキャストネットワークへのユーザアクセスを制限する認証パラメータをクリアするには、特権 EXEC モードで **clear ipv6 multicast aaa authorization** コマンドを使用します。

clear ipv6 multicast aaa authorization [*interface-type interface-number*]

Syntax Description	<i>interface-type interface-number</i>	インターフェイスのタイプと番号。詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
---------------------------	--	---

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines オプションの *interface-type* 引数と *interface-number* 引数なしで **clear ipv6 multicast aaa authorization** コマンドを使用すると、ネットワーク上のすべての認証パラメータがクリアされます。

Examples

次に、IPv6 ネットワーク上に設定されているすべての認証パラメータをクリアする例を示します。

```
デバイス# clear ipv6 multicast aaa authorization FastEthernet 1/0
```

Related Commands	コマンド	説明
	aaa authorization multicast default	IPv6 マルチキャストネットワークへのユーザアクセスを制限するパラメータを設定します。

clear ipv6 nd destination

IPv6 ホストモードの宛先キャッシュのエントリをクリアするには、特権 EXEC モードで **clear ipv6 nd destination** コマンドを使用します。

clear ipv6 nd destination[*vrf vrf-name*]

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
----------------------------	--

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear ipv6 nd destination コマンドは IPv6 ホストモードの宛先キャッシュのエントリをクリアします。**vrf vrf-name** キーワードと引数のペアを使用すると、指定した VRF に関する情報のみがクリアされます。

Examples

次に、IPv6 ホストモードの宛先キャッシュのエントリをクリアする例を示します。

```
デバイス# clear ipv6 nd destination
```

Related Commands

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホストモードを有効にします。

clear ipv6 nd on-link prefix

ルータアドバタイズメント (RA) を通じて学習したオンリンクプレフィックスをクリアするには、特権 EXEC モードで **clear ipv6 nd on-link prefix** コマンドを使用します。

clear ipv6 nd on-link prefix[vrf *vrf-name*]

Syntax Description	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
---------------------------	----------------------------	--

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines RA を通じて学習したローカルに到達可能な IPv6 アドレス (on-link プレフィックス) をクリアするには、**clear ipv6 nd on-link prefix** コマンドを使用します。**vrf** *vrf-name* キーワードと引数のペアを使用すると、指定した VRF に関する情報のみがクリアされます。

Examples

次に、RA を通じて学習したオンリンクプレフィックスをクリアする例を示します。

```
デバイス# clear ipv6 nd on-link prefix
```

Related Commands	コマンド	説明
	ipv6 nd host mode strict	conformant または strict の IPv6 ホストモードを有効にします。

clear ipv6 nd router

ルータアドバタイズメント（RA）を通じて学習したネイバー探索（ND）デバイスのエントリをクリアするには、特権 EXEC モードで **clear ipv6 nd router** コマンドを使用します。

clear ipv6 nd router[vrf *vrf-name*]

Syntax Description

vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
----------------------------	---

Command Modes

特権 EXEC（#）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

RA を通じて学習した ND デバイスをクリアするには **clear ipv6 nd router** コマンドを使用します。**vrf** *vrf-name* キーワードと引数のペアを使用すると、指定した VRF に関する情報のみがクリアされます。

Examples

次に、RA を通じて学習したネイバー探索 ND デバイスのエントリをクリアする例を示します。

```
デバイス# clear ipv6 nd router
```

Related Commands

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホストモードを有効にします。

clear ipv6 neighbors

Virtual Routing and Forwarding (VRF) 以外のインターフェイス上の静的エントリおよびND キャッシュのエントリを除き、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除するには、特権 EXEC モードで **clear ipv6 neighbors** コマンドを使用します。

```
clear ipv6 neighbors [interface type number[ipv6 ipv6-address] | statistics | vrf table-name [ipv6-address | statistics]]
```

```
clear ipv6 neighbors
```

Syntax Description	
interface <i>type number</i>	(任意) 指定したインターフェイスの IPv6 ネイバー探索キャッシュをクリアします。
ipv6 <i>ipv6-address</i>	(任意) 指定したインターフェイス上の指定した IPv6 アドレスに一致する IPv6 ネイバー探索キャッシュをクリアします。
statistics	(任意) IPv6 ネイバー探索エントリのキャッシュをクリアします。
vrf	(任意) バーチャルプライベート ネットワーク (VPN) のルーティングインスタンスまたは転送インスタンスのエントリをクリアします。
<i>table-name</i>	(任意) テーブル名または識別子。値の範囲は 0x0 ~ 0xFFFFFFFF (10 進数では 0 ~ 65535) です。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **clear ipv6 neighbor** コマンドは ND キャッシュのエントリをクリアします。**vrf** キーワードなしにコマンドを発行すると、このコマンドはデフォルトのルーティングテーブルに関連付けられているインターフェイス (**vrf forwarding** ステートメントを持たないインターフェイス) 上の ND キャッシュのエントリをクリアします。**vrf** キーワードを指定してコマンドを発行すると、指定した VRF に関連付けられているインターフェイス上の ND キャッシュのエントリをクリアします。

Examples

次に、静的エントリおよび VRF 以外のインターフェイス上の ND キャッシュのエントリを除き、ネイバー探索キャッシュ内のすべてのエントリを削除する例を示します。

```
デバイス# clear ipv6 neighbors
```

clear ipv6 neighbors

次に、静的エントリおよび VRF 以外のインターフェイス上の ND キャッシュのエントリを除き、イーサネット インターフェイス 0/0 上の IPv6 ネイバー探索キャッシュのすべてのエントリをクリアする例を示します。

```
デバイス# clear ipv6 neighbors interface Ethernet 0/0
```

次に、イーサネット インターフェイス 0/0 上の 2001:0DB8:1::1 のネイバー探索キャッシュのエントリをクリアする例を示します。

```
デバイス# clear ipv6 neighbors interface Ethernet0/0 ipv6 2001:0DB8:1::1
```

次の例では、インターフェイス イーサネット 0/0 が red という VRF と関連付けられています。インターフェイスのイーサネット 1/0 とイーサネット 2/0 は（VRF と関連付けられていないため）デフォルトのルーティング テーブルと関連付けられています。したがって、**clear ipv6 neighbor** コマンドはインターフェイスのイーサネット 1/0 とイーサネット 2/0 上の ND キャッシュのエントリのみをクリアします。インターフェイス イーサネット 0/0 上の ND キャッシュのエントリをクリアするには、**clear ipv6 neighbor vrf red** コマンドを発行する必要があります。

```
interface ethernet0/0
  vrf forward red
  ipv6 address 2001:db8:1::1/64

interface ethernet1/0
  ipv6 address 2001:db8:2::1/64

interface ethernet2/0
  ipv6 address 2001:db8:3::1/64
```

Related Commands

コマンド	説明
ipv6 neighbor	IPv6 ネイバー探索キャッシュのスタティックエントリを設定します。
show ipv6 neighbors	IPv6 ネイバー探索キャッシュ情報を表示します。

clear ipv6 ospf

Open Shortest Path First (OSPF) ルーティングプロセス ID に基づく OSPF 状態をクリアするには、特権 EXEC モードで **clear ipv6 ospf** コマンドを使用します。

clear ipv6 ospf [*process-id*] {**process** | **force-spf** | **redistribution**}

Syntax Description	
<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される数は、OSPF ルーティングプロセスをイネーブルにするときに管理目的で割り当てられた数です。
process	OSPF プロセスを再起動します。
force-spf	最初に OSPF データベースをクリアせずに、最短パス優先 (SPF) アルゴリズムを起動します。
redistribution	OSPF ルート再配布をクリアします。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **process** キーワードを **clear ipv6 ospf** コマンドで使用すると、OSPF データベースはいったんクリアされてから再入力された後、最短パス優先 (SPF) アルゴリズムが実行されます。**force-spf** キーワードを **clear ipv6 ospf** コマンドで使用すると、SPF アルゴリズムが実行される前に OSPF データベースはクリアされません。

1 つの OSPF プロセスのみをクリアするには、*process-id* オプションを使用します。*process-id* オプションを指定しなかった場合、すべての OSPF プロセスがクリアされます。

Examples

次に、OSPF データベースをクリアせずに SPF アルゴリズムを起動する例を示します。

```
デバイス# clear ipv6 ospf force-spf
```

clear ipv6 ospf counters

Open Shortest Path First (OSPF) ルーティングプロセス ID に基づく OSPF 状態をクリアするには、特権 EXEC モードで **clear ipv6 ospf** コマンドを使用します。

clear ipv6 ospf [*process-id*] **counters** [**neighbor** [*neighbor-interface*neighbor-id]]

Syntax Description

<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できません。ここで使用される数は、OSPF ルーティングプロセスをイネーブルにするときに管理目的で割り当てられた数です。
neighbor	(任意) インターフェイスごとまたはネイバー ID ごとのネイバー統計。
<i>neighbor-interface</i>	(任意) ネイバーインターフェイス。
<i>neighbor-id</i>	(任意) ネイバーの IPv6 アドレスまたは IP アドレス。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

指定したインターフェイス上のすべてのネイバーのカウンタをクリアするには、**neighbor neighbor-interface** オプションを使用します。**neighbor neighbor-interface** オプションを使用しないと、すべての OSPF カウンタがクリアされます。

指定したネイバーのカウンタをクリアするには、**neighbor neighbor-id** オプションを使用します。**neighbor neighbor-id** オプションを使用しないと、すべての OSPF カウンタがクリアされます。

Examples

次に、ネイバルータに関する詳細情報を表示する例を示します。

```

デバイス# show ipv6 ospf neighbor detail
Neighbor 10.0.0.1
  In the area 1 via interface Serial19/0
  Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
  Neighbor priority is 1, State is FULL, 6 state changes
  Options is 0x194AE05
  Dead timer due in 00:00:37
  Neighbor is up for 00:00:15
  Index 1/1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec

```

次に、指定したインターフェイス上のすべてのネイバーをクリアする例を示します。

```

デバイス# clear ipv6 ospf counters neighbor s19/0

```

次の例は、**clear ipv6 ospf counters neighbor s19/0** コマンドを使用して以来状態変化がないことを示しています。

```
デバイス# show ipv6 ospf neighbor detail
Neighbor 10.0.0.1
  In the area 1 via interface Serial19/0
  Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
  Neighbor priority is 1, State is FULL, 0 state changes
  Options is 0x194AE05
  Dead timer due in 00:00:39
  Neighbor is up for 00:00:43
  Index 1/1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

コマンド	説明
show ipv6 ospf neighbor	OSPF ネイバー情報をインターフェイスごとに表示します。

clear ipv6 ospf events

Open Shortest Path First (OSPF) ルーティングプロセス ID に基づく IPv6 イベントログカウンタの OSPF をクリアするには、特権 EXEC モードで **clear ipv6 ospf events** コマンドを使用します。

clear ipv6 ospf [*process-id*] **events**

Syntax Description

<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される数は、OSPF ルーティングプロセスをイネーブルにするときに管理目的で割り当てられた数です。
-------------------	--

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

指定した OSPF ルーティングプロセスの IPv6 イベントログカウンタをクリアするには、任意の *process-id* 引数を使用します。*process-id* 引数を使用しなかった場合は、すべてのイベントログカウンタがクリアされます。

Examples

次に、ルーティングプロセス 1 の IPv6 イベントログカウンタの OSPF をクリアする例を示します。

デバイス# **clear ipv6 ospf 1 events**

clear ipv6 pim reset

トポロジテーブルからすべてのエントリを削除し、マルチキャストルーティング情報ベース（MRIB）接続をリセットするには、特権 EXEC モードで **clear ipv6 pim reset** コマンドを使用します。

```
clear ipv6 pim [vrf vrf-name] reset
```

Syntax Description	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
---------------------------	----------------------------	--

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **clear ipv6 pim reset** コマンドを使用すると、PIM-MRIB 接続が切断され、トポロジテーブルがクリアされてから PIM-MRIB 接続が再確立されます。このプロシージャは MRIB を強制的に再同期します。



Caution **clear ipv6 pim reset** コマンドは PIM トポロジテーブルからすべての PIM プロトコル情報をクリアするため、使用する際は注意が必要です。**clear ipv6 pim reset** コマンドは、PIM と MRIB の通信が正常に動作しない場合に使用してください。

Examples

次に、トポロジテーブルからすべてのエントリを削除し、MRIB 接続をリセットする例を示します。

```
デバイス# clear ipv6 pim reset
```

clear ipv6 pim topology

Protocol Independent Multicast (PIM) トポロジテーブルをクリアするには、特権 EXEC モードで **clear ipv6 pim topology** コマンドを使用します。

clear ipv6 pim [**vrf** *vrf-name*] **topology** [*group-name**group-address*]

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。

Command Default

引数を指定しないでこのコマンドを使用すると、PIM トポロジテーブルにあるすべてのグループエントリから PIM プロトコル情報がクリアされます。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、PIM トポロジテーブルにあるすべてのグループエントリから PIM プロトコル情報をクリアします。MRIB テーブルから取得した情報は保持されます。マルチキャストグループを指定した場合は、それらのグループエントリだけがクリアされます。

Examples

次に、PIM トポロジテーブルにあるすべてのグループエントリをクリアする例を示します。

```
デバイス# clear ipv6 pim topology
```

clear ipv6 pim traffic

Protocol Independent Multicast (PIM) トラフィックカウンタをクリアするには、特権 EXEC モードで **clear ipv6 pim traffic** コマンドを使用します。

clear ipv6 pim [vrf vrf-name] traffic

Syntax Description	vrf vrf-name (任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
---------------------------	--

Command Default 引数なしでこのコマンドを使用すると、すべてのトラフィックカウンタがクリアされます。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、PIM トラフィックカウンタをクリアします。 **vrf vrf-name** キーワードと引数を使用すると、それらのカウンタのみがクリアされます。

Examples

次に、すべての PIM トラフィックカウンタをクリアする例を示します。

```
デバイス# clear ipv6 pim traffic
```

clear ipv6 prefix-list

IPv6 プレフィックスリストのエントリのヒットカウントをリセットするには、特権 EXEC モードで **clear ipv6 prefix-list** コマンドを使用します。

clear ipv6 prefix-list [*prefix-list-name*] [*ipv6-prefix/prefix-length*]

Syntax Description

<i>prefix-list-name</i>	(任意) ヒットカウントをクリアするプレフィックスリストの名前。
<i>ipv6-prefix</i>	(任意) ヒットカウントをクリアする IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>/ prefix-length</i>	(オプション) IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。

Command Default

すべての IPv6 プレフィックスリストのヒットカウントがクリアされます。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear ipv6 prefix-list コマンドは、IPv6 固有である点を除いて、**clear ip prefix-list** コマンドに似ています。

ヒットカウントは、特定のプレフィックスリスト エントリに一致する数を示す値です。

Examples

次の例では、ネットワークマスク 2001:0DB8::/35 と一致する、**first_list** という名前のプレフィックスリストのプレフィックスリスト エントリからヒットカウントをクリアします。

```
デバイス# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

Related Commands

コマンド	説明
ipv6 prefix-list	IPv6 プレフィックスリストのエントリを作成します。
ipv6 prefix-list sequence-number	IPv6 プレフィックスリスト内のエントリのシーケンス番号の生成を有効にします。

コマンド	説明
show ipv6 prefix-list	IPv6 プレフィックスリストまたはプレフィックスリストのエントリに関する情報を表示します。

clear ipv6 rip

IPv6 Routing Information Protocol (RIP) ルーティングテーブルからルートを削除するには、特権 EXEC モードで **clear ipv6 rip** コマンドを使用します。

clear ipv6 rip [*name*][*vrf vrf-name*]

clear ipv6 rip [*name*]

Syntax Description

<i>name</i>	(任意) IPv6 RIP プロセスの名前。
vrf <i>vrf-name</i>	(任意) 指定した Virtual Routing and Forwarding (VRF) インスタンスに関する情報をクリアします。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

name 引数を指定すると、指定した IPv6 RIP プロセスのルートのみが IPv6 RIP ルーティングテーブルから削除されます。*name* 引数を指定しないと、すべての IPv6 RIP ルートが削除されます。

IPv6 RIP ルートを表示するには、**show ipv6 rip** コマンドを使用します。

指定した IPv6 RIP プロセスの指定した VRF インスタンスを削除するには、**clear ipv6 rip name vrf vrf-name** コマンドを使用します。

Examples

次に、one という RIP プロセスのすべての IPv6 ルートを削除する例を示します。

```
デバイス# clear ipv6 rip one
```

次に、one という RIP プロセスの vrf1 という IPv6 VRF インスタンスを削除する例を示します。

```
デバイス# clear ipv6 rip one vrf vrf1
```

```
*Mar 15 12:36:17.022: RIPng: Deleting 2001:DB8::/32
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete all next-hops for 2001:DB8::1
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete 2001:DB8::1 from table
*Mar 15 12:36:17.022: [IPv6 RIB Event Handler]IPv6RT[<red>]: Event: 2001:DB8::1, Del, owner
rip, previous None
```

Related Commands

コマンド	説明
debug ipv6 rip	IPv6 RIP ルーティングテーブルの現在の内容を表示します。

コマンド	説明
ipv6 rip vrf-mode enable	IPv6 RIP の VRF 認識型サポートを有効にします。
show ipv6 rip	IPv6 RIP ルーティングテーブルの現在の内容を表示します。

clear ipv6 route

IPv6 ルーティングテーブルからルートを削除するには、特権 EXEC モードで **clear ipv6 route** コマンドを使用します。

```
{clear ipv6 route {ipv6-address|ipv6-prefix/prefix-length} |*}
```

Syntax Description

<i>ipv6-address</i>	テーブルから削除する IPv6 ネットワークアドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>ipv6-prefix</i>	テーブルから削除する IPv6 ネットワーク番号。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>/ prefix-length</i>	IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
*	すべての IPv6 ルートをクリアします。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear ipv6 route コマンドは、IPv6 固有である点を除いて、**clear ip route** コマンドに似ています。

ipv6-address 引数または *ipv6-prefix/prefix-length* 引数を指定した場合は、IPv6 ルーティングテーブルからそのルートが削除されます。* キーワードを指定した場合は、すべてのルートがルーティングテーブルから削除されます（宛先単位の最大伝送ユニット（MTU）キャッシュもクリアされます）。

Examples

次に、IPv6 ネットワーク 2001:0DB8::/35 を削除する例を示します。

```
デバイス# clear ipv6 route 2001:0DB8::/35
```

Related Commands

コマンド	説明
ipv6 route	スタティック IPv6 ルートを確立します。
show ipv6 route	IPv6 ルーティングテーブルの現在の内容を表示します。

clear ipv6 spd

最新の選択的パケット破棄（SPD）の状態遷移をクリアするには、特権 EXEC モードで **clear ipv6 spd** コマンドを使用します。

clear ipv6 spd

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC（#）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear ipv6 spd コマンドは、最新の SPD 状態遷移と傾向履歴データを削除します。

Examples

次に、最新の SPD 状態遷移をクリアする例を示します。

```
デバイス# clear ipv6 spd
```

fhrp delay

First Hop Redundancy Protocol (FHRP) クライアントの初期化の遅延時間を指定するには、インターフェイス コンフィギュレーション モードで **fhrp delay** コマンドを使用します。指定した時間を削除するには、このコマンドの **no** 形式を使用します。

```
fhrp delay {[minimum] [reload] seconds}
no fhrp delay {[minimum] [reload] seconds}
```

Syntax Description

minimum	(任意) インターフェイスが使用可能になった後の遅延時間を設定します。
reload	(任意) デバイスのリロード後の遅延時間を設定します。
<i>seconds</i>	秒単位の遅延時間。範囲は 0 ~ 3600 です。

Command Default

なし

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、FHRP クライアントの初期化の遅延期間を指定する例を示します。

```
Device(config-if)# fhrp delay minimum 90
```

Related Commands

コマンド	説明
show fhrp	ファーストホップ冗長性プロトコル (FHRP) の情報を表示します。

fhrp version vrrp v3

Virtual Router Redundancy Protocol バージョン 3 (VRRPv3) と Virtual Router Redundancy Service (VRRS) をデバイスで有効にするには、グローバルコンフィギュレーションモードで **fhrp version vrrp v3** コマンドを使用します。VRRPv3 と VRRS の設定機能をデバイスで無効にするには、このコマンドの **no** 形式を使用します。

```
fhrp version vrrp v3
no fhrp version vrrp v3
```

Syntax Description

このコマンドにはキーワードまたは引数はありません。

Command Default

VRRPv3 と VRRS 設定はデバイスで有効になっていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

VRRPv3 が使用中の場合、VRRP バージョン 2 (VRRPv2) は使用できません。

Examples

次の例では、トラッキング プロセスは、VRRPv3 グループを使用して IPv6 オブジェクトの状態を追跡するように設定されています。ギガビット イーサネット インターフェイス 0/0/0 の VRRP は、VRRPv3 グループで IPv6 オブジェクトに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス VRRPv3 の IPv6 オブジェクト ステートがダウンになると、VRRP グループのプライオリティは 20 だけ引き下げられます。

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

Related Commands

コマンド	説明
track (VRRP)	VRRPv3 グループを使用したオブジェクトの追跡を有効にします。

ip address dhcp

DHCP からインターフェイスの IP アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ip address dhcp** コマンドを使用します。取得されたいずれかのアドレスを削除するには、このコマンドの **no** 形式を使用します。

ip address dhcp [*client-id interface-type number*] [*hostname hostname*]
no ip address dhcp [*client-id interface-type number*] [*hostname hostname*]

Syntax Description

client-id	(任意) クライアント ID を指定します。デフォルトでは、クライアント識別子は ASCII 値です。 client-id interface-type number オプションは、クライアント識別子を、指定されたインターフェイスの 16 進数 MAC アドレスに設定します。
interface-type	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
number	(任意) インターフェイスまたはサブインターフェイスの番号です。ネットワーク デバイスに対する番号付け構文の詳細については、疑問符 (?) のオンラインヘルプ機能を使用してください。
hostname	(任意) ホスト名を指定します。
hostname	(任意) ホスト名を DHCP オプション 12 フィールドに配置します。この名前は、グローバルコンフィギュレーションモードで入力されたホスト名と同じにする必要はありません。

Command Default

ホスト名は、デバイスのグローバルコンフィギュレーションホスト名です。クライアント識別子は ASCII 値です。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ip address dhcp コマンドを使用すると、インターフェイスは DHCP プロトコルを使用して IP アドレスを動的に学習できます。これはインターネット サービス プロバイダー (ISP) に動的に接続するイーサネットインターフェイスで特に役立ちます。このインターフェイスにダイナミックアドレスを割り当てると、同インターフェイスを使用して、Cisco IOS ネットワーク アドレス変換 (NAT) のポートアドレス変換 (PAT) で、デバイスに接続済みの個別に処理されたネットワークにインターネット アクセスを提供できます。

また **ip address dhcp** コマンドは、ATM ポイントツーポイント インターフェイスと連動し、どのカプセル化方式でも受け入れます。ただし、ATM マルチポイント インターフェイスの場合、

protocol ip inarp インターフェイス コンフィギュレーション コマンドで Inverse ARP を指定し、aa15snap カプセル化タイプのみを使用する必要があります。

一部の ISP の場合、DHCPDISCOVER メッセージに、特定のホスト名と、インターフェイスの MAC アドレスであるクライアント識別子を含める必要があります。**ip address dhcp client-id interface-type number hostname hostname** コマンドは、*interface-type* が、このコマンドが設定されたイーサネットインターフェイスであり、*interface-type number* が ISP によって提供されたホスト名である場合に最も一般的に使用されます。

クライアント識別子 (DHCP オプション 61) には、16 進数または ASCII 値を使用できます。デフォルトでは、クライアント識別子は ASCII 値です。**client-id interface-type number** オプションは、デフォルトの値を上書きし、指定されたインターフェイスの 16 進数 MAC アドレスの使用を強制します。

DHCP サーバから IP アドレスを取得するようシスコ デバイスが設定されている場合、デバイスは、ネットワークの DHCP サーバにデバイスに関する情報を提供する DHCPDISCOVER メッセージを送信します。

ip address dhcp コマンドを使用する場合、オプションキーワードの有無にかかわらず、DHCP オプション 12 フィールド (ホスト名オプション) が DISCOVER メッセージに含まれます。デフォルトでは、オプション 12 で指定されたホスト名は、デバイスのグローバルコンフィギュレーションホスト名になります。ただし、**ip address dhcp hostname hostname** コマンドを使用して、デバイスのグローバルコンフィギュレーションホスト名ではない別の名前を DHCP オプション 12 フィールドに入力することもできます。

no ip address dhcp コマンドは、取得済みの IP アドレスを削除して、DHCPRELEASE メッセージを送信します。

DHCP サーバで必要なものを判別するため、さまざまな設定を試行しなければならない場合があります。下の表に、使用可能なコンフィギュレーション方式と、各方式の DISCOVER メッセージに含まれる情報を示します。

Table 28: コンフィギュレーション方式と生成される **DISCOVER** メッセージの内容

コンフィギュレーション方式	DISCOVER メッセージの内容
ip address dhcp	DISCOVER メッセージのクライアント ID フィールドには「cisco-mac-address -Eth1」が含まれます。 <i>mac-address</i> は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドのデバイスのデフォルト ホスト名を含んでいます。
ip address dhcp hostname hostname	DISCOVER メッセージのクライアント ID フィールドには「cisco-mac-address -Eth1」が含まれます。 <i>mac-address</i> は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドの <i>hostname</i> を含んでいます。

コンフィギュレーション方式	DISCOVER メッセージの内容
ip address dhcp client-id ethernet 1	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドにデバイスのデフォルトホスト名を含んでいます。
ip address dhcp client-id ethernet 1 hostname hostname	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドに <i>hostname</i> を含んでいます。

Examples

次の例では、**ip address dhcp** コマンドがイーサネット インターフェイス 1 に入力されます。次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「*cisco- mac-address -Eth1*」と、オプション 12 フィールドの値 *abc* が含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「*cisco- mac-address -Eth1*」と、オプション 12 フィールドの値 *def* が含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドのイーサネット インターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 *abc* が含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドのイーサネット インターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 *def* が含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

Related Commands

コマンド	説明
ip dhcp pool	Cisco IOS DHCP サーバに DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。

ip address pool (DHCP)

Dynamic Host Configuration Protocol (DHCP) に IP Control Protocol (IPCP) ネゴシエーションからサブネットが入力されるときに、インターフェイスの IP アドレスが自動設定されるようにするには、インターフェイス コンフィギュレーション モードで **ip address pool** コマンドを使用します。インターフェイスの IP アドレスの自動設定を無効にするには、このコマンドの **no** 形式を使用します。

ip address pool *name*
no ip address pool

Syntax Description

<i>name</i>	DHCP プールの名前。インターフェイスの IP アドレスは、 <i>name</i> で指定された DHCP プールから自動設定されます。
-------------	--

Command Default

IP アドレスのプーリングは無効になっています。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デバイスの DHCP プールによって処理する必要のある LAN に接続されている DHCP クライアントが存在する場合、このコマンドを使用して LAN インターフェイスの IP アドレスを自動設定します。DHCP プールは、IPCP サブネット ネゴシエーションによってサブネットを動的に取得します。

Examples

次の例では、GigabitEthernet インターフェイス 1/0/1 の IP アドレスが abc という名前のアドレス プールから自動設定されるように指定します。

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

Related Commands

コマンド	説明
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ip address

インターフェイスのプライマリまたはセカンダリ IP アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除するか、IP 処理を無効にするには、このコマンドの **no** 形式を使用します。

```
ip address ip-address mask [secondary [vrf vrf-name ]]
no ip address ip-address mask [secondary [vrf vrf-name ]]
```

Syntax Description	
<i>ip-address</i>	IP アドレス。
<i>mask</i>	関連する IP サブネットのマスク。
secondary	(任意) 設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 Note セカンダリ アドレスが vrf のキーワードでの VRF テーブルの設定に使用される場合には、 vrf キーワードも指定する必要があります。
vrf	(任意) VRF テーブルの名前 <i>vrf-name</i> 引数は、入力インターフェイスの VRF 名を指定します。

Command Default IP アドレスはインターフェイスに定義されません。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines インターフェイスには、1つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。Cisco IOS ソフトウェアにより生成されるパケットは、必ずプライマリ IP アドレスを使用します。そのため、セグメントのすべてのデバイスとアクセスサーバは、同じプライマリ ネットワーク番号を共有する必要があります。

ホストは、Internet Control Message Protocol (ICMP) マスク要求メッセージを使用して、サブネット マスクを判別できます。デバイスは、ICMP マスク応答メッセージでこの要求に応答できます。

no ip address コマンドを使用して IP アドレスを削除することにより、特定のインターフェイス上の IP 処理を無効にできます。ソフトウェアが、その IP アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラーメッセージを出力します。

オプションの **secondary** キーワードを使用すると、セカンダリアドレスを無制限に指定できます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP プ

ロードキャストおよび Address Resolution Protocol (ARP) 要求は、IP ルーティング テーブルのインターフェイス ルートのように、正しく処理されます。

セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワークセグメントに十分なホストアドレスがない場合。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1つの物理サブネットでは、300 のホストアドレスが必要になります。デバイスまたはアクセス サーバでセカンダリ IP アドレスを使用すると、2つの論理サブネットで1つの物理サブネットを使用できます。
- レベル 2 ブリッジを使用して構築された旧式ネットワークがたくさんある場合。セカンダリアドレスは、慎重に使用することで、サブネット化されたデバイスベース ネットワークへの移行に役立ちます。旧式のブリッジセグメントのデバイスでは、そのセグメントに複数のサブネットがあることを簡単に認識させることができます。
- 1つのネットワークの2つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。サブネットが使用中の場合、この状況は許可されません。このような場合、最初のネットワークは、セカンダリ アドレスを使用している 2 番目のネットワークの上に拡張されます。つまり、上の階層となります。



Note

- ネットワークセグメント上のすべてのデバイスがセカンダリアドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリアドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリアドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。
- Open Shortest Path First (OSPF) アルゴリズムを使用してルーティングする場合は、インターフェイスのすべてのセカンダリアドレスがプライマリアドレスと同じ OSPF エリアにあることを確認してください。
- セカンダリ IP アドレスを設定する場合は、CPU 使用率が高くなるないように、**no ip redirects** コマンドを入力して ICMP リダイレクトメッセージの送信を無効にする必要があります。

Examples

次の例では、192.108.1.27 がプライマリ アドレスで、192.31.7.17 が GigabitEthernet インターフェイス 1/0/1 のセカンダリ アドレスです。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

Related Commands	Command	Description
	match ip route-source	送信元IPアドレスを、VRFで接続されたルートに基づいて設定された必要なルートマップに一致するように指定します。
	route-map	1つのルーティングプロトコルから他のルーティングプロトコルへのルートを再配布するか、またはポリシールーティングを有効にするための条件を定義します。
	set vrf	ポリシーベースルーティングVRFの選択のために、ルートマップ内でVPN VRF選択を有効にします。
	show ip arp	SLIPアドレスが固定ARPテーブルエントリとして表示されるARPキャッシュを表示します。
	show ip interface	IP用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。
	show route-map	静的ルートマップと動的ルートマップを表示します。

ip unnumbered

明示的な IP アドレスをインターフェイスに割り当てることなく、インターフェイスでの IP 処理を有効にするには、インターフェイス コンフィギュレーションモードまたはサブインターフェイス コンフィギュレーションモードで **ip unnumbered** コマンドを使用します。インターフェイスで IP 処理を無効にするには、このコマンドの **no** 形式を使用します。

```
ip unnumbered type number [ poll ][ point-to-point ]
no ip unnumbered [ type number ]
```

Syntax Description

type	インターフェイスのタイプ。詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
number	インターフェイスまたはサブインターフェイスの番号。ネットワークデバイスに対する番号付けシンタックスの詳細については、疑問符 (?) のオンラインヘルプ機能を使用してください。
poll	(任意) IP 接続ホストのポーリングを有効にします。
point-to-point	(任意) ポイントツーポイント接続を有効にします。

Command Default

番号が付いていないインターフェイスはサポートされません。

Command Modes

インターフェイス コンフィギュレーション (config-if)
サブインターフェイス コンフィギュレーション (config-subif)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.8.1a	このコマンドが導入されました。

Usage Guidelines

アンナンバードインターフェイスがパケットを生成する場合 (たとえば、ルーティングアップデートのため)、IP パケットの送信元アドレスとして指定されているインターフェイスのアドレスが使用されます。また、アンナンバードインターフェイスを介してアップデートを送信するルーティングプロセスを判別する場合、指定されたインターフェイスの IP アドレスが使用されません。

このコマンドには次の制限が適用されます。

- High-Level Data Link Control (HDLC)、PPP、Link Access Procedure Balanced (LAPB)、フレームリレーカプセル化、および Serial Line Internet Protocol (SLIP) を使用するシリアルインターフェイス、およびトンネルインターフェイスはアンナンバードで使用できます。
- インターフェイスにはアドレスがないため、**ping EXEC** コマンドを使用してインターフェイスがアップ状態かどうかを確認することはできません。簡易ネットワーク管理プロトコル (SNMP) は、インターフェイス ステータスのリモート監視に使用できます。

- **ip unnumbered** コマンドを使用して、IP アドレスが割り当てられているシリアルインターフェイスを介して Cisco IOS イメージをネットブートすることはできません。
- IP セキュリティ オプションは、アンナンバード インターフェイス上でサポートできません。

type および *number* 引数を使用して指定されたインターフェイスが、有効になっている必要があります (**show interfaces** コマンドの出力に「up」と表示)。

シリアル回線を介して Intermediate System-to-Intermediate System (IS-IS) を設定する場合は、シリアルインターフェイスをアンナンバードとして設定する必要があります。この設定により、各インターフェイスで IP アドレスは必須でないと規定している RFC 1195 に準拠できます。



Note さまざまな主要なネットワーク（またはメジャーネット）間でアンナンバードシリアル回線を使用する場合、特別な注意が必要です。リンクの両端で、アンナンバードとして指定したインターフェイスに異なるメジャーネットが割り当てられている場合、シリアル回線で実行されているルーティングプロトコルはサブネット情報をアドバタイズすることはできません。

Examples

次に、イーサネット 0 のアドレスを最初のシリアルインターフェイスに割り当てる例を示します。

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
!
Device(config-if)# interface serial 0
Device(config-if)# ip unnumbered ethernet 0
```

次に、イーサネット VLAN サブインターフェイス 3/0.2 を IP アンナンバードサブインターフェイスとして設定する例を示します。

```
Device(config)# interface ethernet 3/0.2
Device(config-subif)# encapsulation dot1q 200
Device(config-subif)# ip unnumbered ethernet 3/1
```

次に、5/1.1 ~ 5/1.4 の範囲のファストイーサネット サブインターフェイスを IP アンナンバードサブインターフェイスとして設定する例を示します。

```
Device(config)# interface range fastethernet5/1.1 - fastethernet5/1.4
Device(config-if-range)# ip unnumbered ethernet 3/1
```

次に、ギガビットイーサネット インターフェイスでポーリングを有効にする例を示します。

```
Device(config)# interface loopback0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
!
Device(config-if)# ip unnumbered gigabitethernet 3/1
Device(config-if)# ip unnumbered loopback0 poll
```

ip wccp

サービスグループに参加できるように、指定した Web Cache Communication Protocol (WCCP) サービスのサポートを有効にするには、グローバル コンフィギュレーション モードで **ip wccp** コマンドを使用します。サービスグループを無効にするには、このコマンドの **no** 形式を使用します。

```
ip wccp [ vrf vrf-name ] { web-cache service-number } [ service-list service-access-list ] [
mode { open | closed } ] [ group-address multicast-address ] [ redirect-list access-list ] [
group-list access-list ] [ password [ 0 | 7 ] password ]
no ip wccp [ vrf vrf-name ] { web-cache service-number } [ service-list service-access-list ]
[ mode { open | closed } ] [ group-address multicast-address ] [ redirect-list access-list ]
[ group-list access-list ] [ password [ 0 | 7 ] password ]
```

Syntax Description

vrf <i>vrf-name</i>	(任意) サービスグループに関連付ける Virtual Routing and Forwarding インスタンス (VRF) を指定します。
web-cache	Web キャッシュ サービスを指定します (WCCP バージョン 1 とバージョン 2)。 Note Web キャッシュはサービスの 1 つとしてカウントされます。サービスの最大数 (<i>service-number</i> 引数で割り当てられたサービスを含む) は 256 です。
<i>service-number</i>	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ~ 254 の範囲で指定できます。サービスの最大数 (web-cache キーワードで指定する Web キャッシュ サービスを含む) は 256 です。 Note キャッシュクラスタで Cisco Cache Engine が使用されている場合、リバースプロキシサービスは値 99 で指定されます。
service-list <i>service-access-list</i>	(任意) サービスと一致するパケットを定義する名前付き拡張 IP アクセスリストを指定します。
mode open	(任意) サービスを開いていると見なします。これがデフォルト サービス モードです。
mode closed	(任意) サービスが閉じていると見なします。
group-address <i>multicast-address</i>	(任意) WCCP サービスグループと通信するマルチキャスト IP アドレスを指定します。マルチキャストアドレスは、デバイスが使用してリダイレクトされたメッセージを受信する Web キャッシュを決定します。
redirect-list <i>access-list</i>	(任意) このサービスグループにリダイレクトされるトラフィックを制御するアクセスリストを指定します。 <i>access-list</i> 引数は、アクセスリストを指定する 64 文字以下の長さの文字列 (名前または番号) で構成する必要があります。

group-list <i>access-list</i>	(任意) サービスグループへの参加を許可する Web キャッシュを決定するアクセスリストを指定します。 <i>access-list</i> 引数には、標準または拡張アクセスリストの番号または名前を指定します。
password [0 7] <i>password</i>	(任意) サービスグループから受信したメッセージにメッセージダイジェストアルゴリズム 5 (MD5) 認証を指定します。認証で受け入れられなかったメッセージは廃棄されます。暗号化タイプには 0 ~ 7 のタイプを指定できます。0 は暗号化されないことを、7 は独自の暗号化を示します。 <i>password</i> 引数の長さは最大 8 文字です。

Command Default WCCP サービスがデバイスでイネーブルにされていません。

Command Modes グローバル コンフィギュレーション (config)

リリース	変更内容
	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.6.1	vrf キーワードと <i>vrf-name</i> 引数のペアが追加されました。

Usage Guidelines シスコエクスプレスフォワーディングスイッチングがイネーブルのとき、WCCP の透過的キャッシングはネットワーク アドレス変換 (NAT) をバイパスします。この状況に対処するには、発信方向で WCCP 透過キャッシングを設定し、コンテンツエンジンインターフェイスで Cisco Express Forwarding スwitching を有効にし、**ip wccp web-cache redirect out** コマンドを指定します。キャッシュに面するデバイスインターフェイスで **ip wccp redirect exclude in** コマンドを指定し、内部インターフェイスの着信方向に WCCP を設定します。この設定は、そのインターフェイスに到着したパケットのリダイレクションを回避します。

サービスグループを設定するときにリダイレクトリストを含めることもできます。指定されたリダイレクトリストは、NAT (送信元) IP アドレスを含むパケットを拒否して、リダイレクションを阻止します。

このコマンドは、指定されたサービス番号または Web キャッシュサービス名のサポートをイネーブルまたはディセーブルにするようデバイスに指示します。サービス番号は 0 ~ 254 の範囲で指定できます。サービス番号または名前がイネーブルになると、デバイスはサービスグループの確立に参加できます。



Note すべての WCCP パラメータを単一の IP WCCP コマンドに含める必要があります。例: **ip wccp 61 redirect-list 10 password password**。

vrf *vrf-name* キーワードと引数のペアは任意です。サービスグループに関連付ける VRF を指定できます。次に、Web キャッシュ サービス名またはサービス番号を指定できます。

同じサービス (Web キャッシュまたはサービス番号) を他の VRF テーブルで設定できます。各サービスは個別に動作します。

no ip wccp コマンドが入力されると、デバイスはサービスグループへの参加を終了し、引き続きサービスが設定されているインターフェイスがなければ領域の割り当てを解除し、他のサービスが設定されていない場合は WCCP タスクを終了します。

web-cache に続くキーワードと *service-number* 引数はオプションで、任意の順序で指定できますが、1 回しか指定できません。以降の各項で、このコマンドのオプション形式それぞれの特定の使用方法について概説します。

ip wccp [vrf vrf-name] {web-cache | service-number} group-address multicast-address

デバイスと連動するマルチキャストアドレスをセットアップするように WCCP グループアドレスを設定し、Web キャッシュを使用して WCCP プロトコルメッセージを交換できます。このようなアドレスを使用する場合、IP マルチキャストルーティングを有効にし、設定済みのグループ（マルチキャスト）アドレスを使用するメッセージを正しく受信できるようにする必要があります。

このオプションは、このグループアドレスで受信した「Here I Am」メッセージに対する「I See You」応答を結合するために、指定されたマルチキャスト IP アドレスを使用するようにデバイスに指示します。また、応答はグループアドレスに送信されます。デフォルトではグループアドレスは設定されていないため、すべての「Here I Am」メッセージにユニキャスト応答が返されません。

ip wccp [vrf vrf-name] {web-cache | service-number} redirect-list access-list

このオプションは、サービス名で指定されたサービスグループの Web キャッシュにリダイレクトされるトラフィックの制御にアクセスリストを使用するようにデバイスに指示します。*access-list* 引数には、標準または拡張アクセスリストの番号または名前を指定します。アクセスリストは、リダイレクトを許可されるトラフィックを指定します。デフォルトでは、リダイレクトリストは設定されません（すべてのトラフィックがリダイレクトされます）。

WCCP では、次のプロトコルとポートが、いかなるアクセスリストによってもフィルタリングされないようにする必要があります。

- UDP（プロトコル タイプ 17）ポート 2048。このポートを使用してシグナリングを制御します。このタイプのトラフィックをブロックすることで、WCCP によるデバイスと Web キャッシュ間での接続の確立を阻止します。
- Generic Routing Encapsulation（GRE）（プロトコル タイプ 47 カプセル化フレーム）。このタイプのトラフィックをブロックすることで、代行受信したパケットの表示を阻止します。

ip wccp [vrf vrf-name] {web-cache | service-number} group-list access-list

このオプションは、指定したサービスグループへの参加が許可される Web キャッシュの制御にアクセスリストを使用するようにデバイスに指示します。*access-list* 引数には、標準または拡張アクセスリストの番号、または任意のタイプの名前付きアクセスリストの名前を指定します。アクセスリスト自体は、サービスグループへの参加を許可される Web キャッシュを指定します。デフォルトでは、グループリストは設定されていないため、すべての Web キャッシュがサービスグループに参加する可能性があります。



Note `ip wccp {web-cache | service-number} group-list` コマンドの構文は、`ip wccp {web-cache | service-number} group-listen` コマンドと似ていますが、これらはまったく別のコマンドです。`ip wccp group-listen` コマンドは、キャッシュクラスタからのマルチキャスト通知を受信するようインターフェイスを設定するのに使用する、インターフェイスコンフィギュレーションコマンドです。

`ip wccp [vrf vrf-name] web-cache | service-number} password password`

このオプションは、指定したサービス名で、指定したサービスグループから受信したメッセージのMD5認証を使用するようにデバイスに指示します。この形式のコマンドを使用すると、デバイス上にパスワードを設定できます。また、各 Web キャッシュ上に同じパスワードを個別に設定する必要があります。パスワードは最大8文字を使用できます。デバイスで認証がイネーブルになっているとき、認証されないメッセージは廃棄されます。デフォルトは認証パスワードは設定されておらず、認証はディセーブルになっています。

`ip wccp service-number service-list service-access-list mode closed`

機能処理を適用する目的で、外部仲介デバイスに対する WCCP パケットの代行受信とリダイレクションが Cisco IOS ソフトウェアで利用できないアプリケーションでは、中間デバイスが利用できないときにアプリケーションのパケットをブロックする必要があります。このブロックは、クローズドサービスと呼ばれます。デフォルトでは、WCCP はオープンサービスとして動作します。この場合、中間デバイスがなくても、クライアントとサーバ間の通信は正常に進行します。**service-list** キーワードを使用できるのは、クローズドモードサービスの場合だけです。WCCP サービスをクローズドに設定すると、WCCP が、トラフィックを受信するためのクライアントアプリケーションが登録されていないパケットを破棄します。アプリケーションプロトコルタイプまたはポート番号を登録するには、**service-list** キーワードと *service-access-list* 引数を使用します。

サービスリスト内のサービスの定義と WCCP プロトコルを介して受信した宛て先が競合する場合、次のような警告メッセージが表示されます。

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client 10.1.1.13
```

サービスリストの定義に競合がある場合、WCCP プロトコルメッセージを介して受信した外部定義よりも設定した定義が優先されます。

Examples

次に、マルチキャストアドレス 239.0.0.0 を使用して、WCCP 逆プロキシサービスを実行するように `device` を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip multicast-routing
Device(config)# ip wccp 99 group-address 239.0.0.0
Device(config)# interface ethernet 0
Device(config-if)# ip wccp 99 group-listen
```

次に、宛て先が 10.168.196.51 以外の Web 関連パケットを Web キャッシュにリダイレクトするように `device` を設定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# access-list 100 deny ip any host 10.168.196.51
Device(config)# access-list 100 permit ip any any
Device(config)# ip wccp web-cache redirect-list 100
Device(config)# interface ethernet 0
Device(config-if)# ip wccp web-cache redirect out

```

次に、ネットワーク 10.0.0.0 からのトラフィックがファストイーサネットインターフェイス 0/0 を離れないようにアクセスリストを設定する例を示します。アウトバウンドアクセスコントロールリスト (ACL) チェックが有効になっているため、WCCP はそのトラフィックをリダイレクトしません。WCCP は、パケットのリダイレクト前に、ACL に対してパケットをチェックします。

```

Device> enable
Device# configure terminal
Device(config)# ip wccp web-cache
Device(config)# ip wccp check acl outbound
Device(config)# interface fastethernet0/0
Device(config-if)# ip access-group 10 out
Device(config-if)# ip wccp web-cache redirect out
Device(config-if)# access-list 10 deny 10.0.0.0 0.255.255.255
Device(config-if)# access-list 10 permit any

```

アウトバウンド ACL チェックが無効になっている場合、ネットワーク 10.0.0.0 からの HTTP パケットはキャッシュにリダイレクトされます。ネットワーク管理者がその動作が行われないようにする場合、そのネットワーク アドレスを持つユーザは Web ページを取得できることがあります。

次に、閉じられた WCCP サービスを設定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# ip wccp 99 service-list access1 mode closed

```



Note

- 複数のパラメータが必要な場合、`ip wccp [vrf vrf-name] web-cache | service-number` の下のすべてのパラメータを、1 つのコマンドとして設定する必要があります。
- 異なるパラメータを指定してコマンドを再発行すると、既存のパラメータが削除され、新しいパラメータが設定されます。

次に、複数のパラメータを 1 つのコマンドとして設定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# ip wccp 61 group-address 10.0.0.1 password 0 password mode closed
redirect-list 121

```

Related Commands

コマンド	説明
ip wccp check services all	すべての WCCP サービスをイネーブルにします。
ip wccp group listen	デバイスでインターフェイスを設定して、WCCP の IP マルチキャストパケットの受信をイネーブルまたはディセーブルにします。
ip wccp redirect exclude in	インターフェイスでのリダイレクトの除外をイネーブルにします。
ip wccp redirect out	発信方向のインターフェイスにリダイレクションを設定します。
ip wccp version	デバイスで使用する WCCP のバージョンを指定します。
show ip wccp	WCCP に関連するグローバル統計情報を表示します。

ipv6 access-list

IPv6 アクセスリストを定義してデバイスを IPv6 アクセスリスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。アクセスリストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*
no ipv6 access-list *access-list-name*

Syntax Description

<i>access-list-name</i>	IPv6 アクセスリスト名。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
-------------------------	--

Command Default

IPv6 アクセスリストは定義されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 access-list コマンドは、IPv6 固有である点を除いて、**ip access-list** コマンドに似ています。

標準的な IPv6 ACL 機能は、送信元アドレスと宛先アドレスに基づくトラフィック フィルタリングの他に、IPv6 オプションヘッダーに基づくトラフィックのフィルタリングと、より詳細な制御を行うための任意の上位層プロトコル情報のフィルタリング (IPv4 での拡張 ACL と同様な機能) をサポートしています。IPv6 ACL は、グローバルコンフィギュレーションモードで **ipv6 access-list** コマンドを使用することで定義され、その許可と拒否の条件は IPv6 アクセスリスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用することで設定されます。**ipv6 access-list** コマンドを設定すると、デバイスは IPv6 アクセスリスト コンフィギュレーション モードになり、デバイスプロンプトは Device(config-ipv6-acl)# に変わります。IPv6 アクセスリスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。



Note IPv6 ACL は一意な名前によって定義されます (IPv6 は番号付けされた ACL をサポートしません)。IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

後位互換性を得るため、グローバル コンフィギュレーション モードでの **ipv6 access-list** コマンドと **deny** キーワードおよび **permit** キーワードの組み合わせは現在もサポートされていますが、グローバル コンフィギュレーション モードでの **deny** 条件と **permit** 条件は IPv6 アクセスリスト コンフィギュレーション モードに変換されます。

IPv6 オプション ヘッダーおよび任意の上位層プロトコル タイプ情報に基づく IPv6 トラフィックのフィルタリングの詳細については、`deny (IPv6)` コマンドおよび `permit (IPv6)` コマンドを参照してください。変換された IPv6 ACL の設定例については、「例」の項を参照してください。



Note IPv6 ACL にはそれぞれ、最後に一致した条件として、暗黙の `permit icmp any any nd-na` ステートメント、`permit icmp any any nd-ns` ステートメント、および `deny ipv6 any any` ステートメントがあります（前の2つの一致条件は、ICMPv6 ネイバー探索を許可します）。1つの IPv6 ACL には、暗黙の `deny ipv6 any any` ステートメントを有効にするために少なくとも1つのエントリが含まれている必要があります。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。



Note アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

IPv6 ACL を IPv6 インターフェイスに適用するには、`access-list-name` 引数を指定して `ipv6 traffic-filter` インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ACL をデバイスとの着信および発信 IPv6 仮想端末接続に適用するには、`access-list-name` 引数を指定して、`ipv6 access-class` ライン コンフィギュレーション コマンドを使用します。



Note `ipv6 traffic-filter` コマンドでインターフェイスに適用される IPv6 ACL は、デバイスによって発信されたトラフィックではなく、転送されたトラフィックをフィルタ処理します。



Note このコマンドを使用して、ブートストラップルータ（BSR）の候補のランデブーポイント（RP）（`ipv6 pim bsr candidate rp` コマンドを参照）または静的 RP（`ipv6 pim rp-address` コマンドを参照）とすでに関連付けられている ACL を変更する場合は、PIM SSM グループアドレスの範囲（FF3x::/96）と重複している、追加したアドレス範囲は無視されます。警告メッセージが生成され、重複しているアドレス範囲は ACL に追加されますが、それらは設定した BSR の候補の RP や静的 RP のコマンドの操作には影響を与えません。

重複する `remark` ステートメントは IPv6 アクセス コントロール リストからは設定できなくなりました。各 `remark` ステートメントは個別のエンティティであるため、それぞれが固有であることが必要です。

Examples

次に、Cisco IOS Release 12.0(23)S 以降のリリースを実行するデバイスでの例を示します。次に、list1 という名前の IPv6 ACL を設定し、デバイスを IPv6 アクセスリスト コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

次に、Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、または 12.0(22)S での例を示します。この例では、list2 という IPv6 ACL を設定し、ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用します。特に、最初の ACL エントリは、ネットワーク FEC0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカルプレフィックス FEC0:0:0:2 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。2 番目の ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。2 番目のエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

Cisco IOS Release 12.0(23)S 以降のリリースを実行しているデバイスに同じ設定が入力されていた場合、その設定は次のように IPv6 アクセスリスト コンフィギュレーション モードに変換されます。

```
ipv6 access-list list2
  deny FEC0:0:0:2::/64 any
  permit ipv6 any any
interface ethernet 0
  ipv6 traffic-filter list2 out
```



Note IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセスリスト コンフィギュレーション モードに変換される **permit any any** ステートメントおよび **deny any any** ステートメントでプロトコル タイプとして自動的に設定されます。



Note 暗黙の deny 条件に依存しているか、またはトラフィックをフィルタ処理するために **deny any any** ステートメントを指定した Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、または 12.0(22)S を実行しているデバイスに定義されている IPv6 ACL には、プロトコル パケット（ネイバー探索プロトコルに関連付けられたパケットなど）のフィルタリングを回避するためのリンクローカルとマルチキャストアドレスの **permit** ステートメントを含める必要があります。さらに、**deny** ステートメントを使用してトラフィックをフィルタ処理する IPv6 ACL では、**permit any any** ステートメントをリスト内の最後のステートメントとして使用する必要があります。



Note IPv6 デバイスは、送信元アドレスまたは宛先アドレスのいずれかとしてリンクローカルアドレスを持つ IPv6 パケットを別のネットワークに転送しません（パケットの送信元インターフェイスは、パケットの宛先インターフェイスとは異なります）。

Related Commands

コマンド	説明
deny (IPv6)	IPv6 アクセス リストに拒否条件を設定します。
ipv6 access-class	IPv6 アクセス リストに基づいて、デバイスとの間の着信接続と発信接続をフィルタ処理します。
ipv6 pim bsr candidate rp	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ipv6 pim rp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit (IPv6)	IPv6 アクセス リストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセスリストの内容を表示します。

ipv6 address-validate

IPv6 アドレス検証をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 address-validate** を使用します。IPv6 アドレス検証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 address-validate
no ipv6 address-validate

Command Default このコマンドは、デフォルトでイネーブルになっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

Usage Guidelines **ipv6 address-validate** コマンドは、割り当てられた IPv6 アドレスのインターフェイス識別子が RFC5453 で規定されている予約済み IPv6 インターフェイス識別子の範囲に含まれていないかどうかを検証するために使用します。割り当てられた IPv6 アドレスのインターフェイス識別子が予約済みの範囲に含まれている場合は、新しい IPv6 アドレスが割り当てられます。

検証されるのは、自動設定されたアドレスと DHCPv6 によって設定されたアドレスのみです。



Note **no ipv6-address validate** コマンドを使用すると、IPv6 アドレス検証がディセーブルになり、予約済み IPv6 インターフェイス識別子の範囲に含まれるインターフェイス識別子を使用した IPv6 アドレスの割り当てが可能になります。このコマンドを使用することは推奨しません。

この **ipv6-address validate** コマンドの構文を完成させるために CLI ヘルプ (?) を使用する場合は、コマンドの 8 文字以上を入力する必要があります。入力が 8 文字未満だと、コマンドはインターフェイス コンフィギュレーション モードの **no ipv6 address** コマンドと競合します。

Examples

次に、IPv6 アドレス検証が **no ipv6-address validate** コマンドを使用してディセーブルにされた場合に再度イネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 address-validate
```

ipv6 cef

Cisco Express Forwarding for IPv6 を有効にするには、グローバル コンフィギュレーション モードで **ipv6 cef** コマンドを使用します。Cisco Express Forwarding for IPv6 を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 cef
no ipv6 cef

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

デフォルトでは、Cisco Express Forwarding for IPv6 は無効になっています。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 cef コマンドは、IPv6 固有である点を除いて、**ip cef** コマンドに似ています。

ipv6 cef コマンドは Cisco 12000 シリーズのインターネットルータでは利用できません。これは、Distributed Cisco Express Forwarding for IPv6 モードでのみこの分散型プラットフォームが動作するためです。



Note **ipv6 cef** コマンドはインターフェイス コンフィギュレーション モードではサポートされていません。



Note 一部の分散アーキテクチャプラットフォームで、Cisco Express Forwarding for IPv6 と Distributed Cisco Express Forwarding for IPv6 の両方がサポートされています。分散型プラットフォーム上に Cisco Express Forwarding for IPv6 が設定されている場合、Cisco Express Forwarding スイッチングがルートプロセッサ (RP) によって実行されます。



Note **ipv6 cef** グローバル コンフィギュレーション コマンドを使用して Cisco Express Forwarding for IPv6 を有効にする前に、**ip cef** グローバル コンフィギュレーション コマンドを使用して Cisco Express Forwarding for IPv4 を有効にする必要があります。

Cisco Express Forwarding for IPv6 は、Cisco Express Forwarding for IPv4 と同様に機能し、同じメモリットを提供する高度なレイヤ 3 スイッチング テクノロジーです。Cisco Express Forwarding for IPv6

は、Web ベースアプリケーションやインタラクティブセッションに関連付けられている、ダイナミックでトポロジ的に分散されたトラフィックパターンを使用して、ネットワークのパフォーマンスと拡張性を最適化します。

Examples

次に、標準的な Cisco Express Forwarding for IPv4 の動作を有効にしてから、標準的な Cisco Express Forwarding for IPv6 の動作をデバイス上でグローバルに有効にする例を示します。

```
デバイス(config)# ip cef
デバイス(config)# ipv6 cef
```

Related Commands

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチング キャッシュの使用を制御します。
ipv6 cef accounting	Cisco Express Forwarding for IPv6 と Distributed Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを有効にします。
ipv6 cef distributed	IPv6 での分散型シスコエクスプレスフォワーディングをイネーブルにします。
show cef	ラインカードがドロップしたパケットを表示し、高速伝送されなかったパケットを表示します。
show ipv6 cef	IPv6 FIB 内のエントリを表示します。

ipv6 cef accounting

Cisco Express Forwarding for IPv6 と Distributed Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを有効にするには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **ipv6 cef accounting** コマンドを使用します。Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを無効にするには、このコマンドの **no** 形式を使用します。

```
ipv6 cef accounting accounting-types
no ipv6 cef accounting accounting-types
```

インターフェイス コンフィギュレーション モードを介した特定の Cisco Express Forwarding アカウンティング情報

```
ipv6 cef accounting non-recursive {external | internal}
no ipv6 cef accounting non-recursive {external | internal}
```

Syntax Description

<i>accounting-types</i>	<p><i>accounting-types</i> 引数は、次のキーワードの 1 つ以上で置換する必要があります。必要に応じて、他のキーワードのいずれかまたは全部をこのキーワードに続けることはできますが、各キーワードを使用できるのは 1 回のみです。</p> <ul style="list-style-type: none"> • load-balance-hash : ロードバランシングハッシュ バケットカウンタを有効にします。 • non-recursive : 非再帰的なプレフィックスを介したアカウンティングを有効にします。 • per-prefix : 宛先（またはプレフィックス）へのパケット数とバイト数のコレクションの高速転送を有効にします。 • prefix-length : プレフィックス長を介したアカウンティングを有効にします。
non-recursive	<p>非再帰的なプレフィックスを介したアカウンティングを有効にします。</p> <p>このキーワードは、別のキーワードを入力した後に、必要に応じてグローバル コンフィギュレーション モードで使用します。 <i>accounting-types</i> 引数を参照してください。</p>
external	<p>非再帰的な外部ビン内の入力トラフィックをカウントします。</p>
internal	<p>非再帰的な内部ビン内の入力トラフィックをカウントします。</p>

Command Default

デフォルトでは、Cisco Express Forwarding for IPv6 のネットワーク アカウンティングは無効になっています。

Command Modes

グローバル コンフィギュレーション (config)

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 cef accounting コマンドは、IPv6 固有である点を除いて、**ip cef accounting** コマンドに似ています。

Configuring Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを設定すると、ネットワーク内の IPv6 トラフィック パターンについて Cisco Express Forwarding の統計情報を収集できます。

ipv6 cef accounting コマンドをグローバル コンフィギュレーション モードで使用して Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを有効にすると、Cisco Express Forwarding for IPv6 モードが有効になっている場合のルート プロセッサ (RP) と、Distributed Cisco Express Forwarding for IPv6 が有効になっている場合のラインカードで アカウンティング情報が収集されません。**show ipv6 cef EXEC** コマンドを使用すると、収集された アカウンティング情報を表示できます。

直接接続されたネクストホップがあるプレフィックスの場合、**non-recursive** キーワードはプレフィックスを介したパケットとバイトのコレクションの高速伝送を可能にします。**ipv6 cef accounting** コマンドに別のキーワードを入力した後に、グローバル コンフィギュレーション モードでこのコマンドを使用する場合、このキーワードはオプションです。

インターフェイス コンフィギュレーション モードでは、このコマンドをグローバル コンフィギュレーション コマンドと併せて使用する必要があります。インターフェイス コンフィギュレーション コマンドでは、統計情報の累積に 2 つの異なるビン (内部または外部) を指定できます。デフォルトでは、内部ビンが使用されます。統計情報は **show ipv6 cef detail** コマンドを介して表示されます。

宛先ごとのロード バランシングでは、一連の利用可能パスが分散している一連の 16 ハッシュ バケットを使用します。使用するパスが含まれているバケットを選択するには、パケットの特定の プロパティで動作するハッシュ関数を適用します。送信元と宛先の IP アドレスは、宛先ごとのロード バランシング用のバケットを選択するために使用するプロパティです。ハッシュバケットごとのカウンタを有効にするには、**load-balance-hash** キーワードと **ipv6 cef accounting** コマンドを使用します。ハッシュバケットごとのカウンタを表示するには、**show ipv6 cef prefix internal** コマンドを入力します。

Examples

次に、直接接続されたネクストホップを持つプレフィックスに IPv6 アカウンティング情報の収集を有効にする例を示します。

```
デバイス(config)# ipv6 cef accounting non-recursive
```

Related Commands

Command	Description
ip cef accounting	Cisco Express Forwarding ネットワーク アカウンティング (IPv4 の場合) を有効にします。
show cef	パケットに関する情報を表示します。 forwarded by Cisco Express Forwarding.
show ipv6 cef	IPv6 FIB 内のエントリを表示します。

ipv6 cef distributed

Distributed Cisco Express Forwarding for IPv6 を有効にするには、グローバル コンフィギュレーション モードで **ipv6 cef distributed** コマンドを使用します。Cisco Express Forwarding for IPv6 を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 cef distributed
no ipv6 cef distributed

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトでは、Distributed Cisco Express Forwarding for IPv6 は無効になっています。

Command Modes グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 cef distributed コマンドは、IPv6 固有である点を除いて、**ip cef distributed** コマンドに似ています。

ipv6 cef distributed をグローバル コンフィギュレーション モードで使用し、Distributed Cisco Express Forwarding for IPv6 をルータでグローバルに有効にすると、IPv6 パケットの Cisco Express Forwarding 処理をルートプロセッサ (RP) から分散型アーキテクチャのプラットフォームのラインカードに配信します。



Note ルータ上で Distributed Cisco Express Forwarding IPv6 トラフィックを転送するには、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用してルータ上に IPv6 ユニキャスト データグラムをグローバルに設定し、**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用してインターフェイス上に IPv6 アドレスと IPv6 処理を設定します。



Note Distributed Cisco Express Forwarding for IPv4 は、**ip cef distributed** グローバル コンフィギュレーション コマンドを使用して Distributed Cisco Express Forwarding for IPv6 を有効にする前に、**ipv6 cef distributed** グローバル コンフィギュレーション コマンドを使用して有効にする必要があります。

Cisco Express Forwarding は、高度なレイヤ 3 IP スイッチング テクノロジーです。Cisco Express Forwarding は、Web ベース アプリケーションとインタラクティブセッションに関連付けられているダイナミックで、トポロジ的に分散したトラフィックパターンを持つネットワークのパフォーマンスと拡張性を最適化します。

Examples

次に、Distributed Cisco Express Forwarding for IPv6 動作を有効にする例を示します。

```
デバイス(config)# ipv6 cef distributed
```

Related Commands

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチングキャッシュの使用を制御します。
show ipv6 cef	IPv6 FIB 内のエントリを表示します。

ipv6 cef load-sharing algorithm

Cisco Express Forwarding ロードバランシング アルゴリズムを IPv6 に選択するには、グローバル コンフィギュレーション モードで **ipv6 cef load-sharing algorithm** コマンドを使用します。デフォルトのユニバーサル ロードバランシング アルゴリズムに戻るには、このコマンドの **no** 形式を使用します。

ipv6 cef load-sharing algorithm {original | universal [*id*]}
no ipv6 cef load-sharing algorithm

Syntax Description

original	送信元および宛先のハッシュに基づいて、ロードバランス アルゴリズムを元のアルゴリズムに設定します。
universal	送信元ハッシュ、宛先ハッシュ、ID ハッシュを使用するユニバーサル アルゴリズムに、ロードバランシング アルゴリズムを設定します。
<i>id</i>	(任意) 16 進数形式の固定識別子。

Command Default

ユニバーサルロードバランシングアルゴリズムがデフォルトで選択されています。ロードバランシング アルゴリズムに固定識別子を設定しなかった場合、デバイスは固有 ID を自動的に生成します。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 cef load-sharing algorithm コマンドは、IPv6 固有である点を除いて、**ip cef load-sharing algorithm** コマンドに似ています。

Cisco Express Forwarding for IPv6 のロードバランシング アルゴリズムはユニバーサルモードに設定され、ネットワーク上の各デバイスは送信元アドレスと宛先アドレスのペアごとに異なるロード共有を決定できます。

Examples

次に、Cisco Express Forwarding の IPv6 用の元のロードバランシング アルゴリズムを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 cef load-sharing algorithm original
```

Related Commands

コマンド	説明
ip cef load-sharing algorithm	Cisco Express Forwarding のロードバランシング アルゴリズムを選択します (IPv4 の場合)。

ipv6 cef optimize neighbor resolution

Cisco Express Forwarding for IPv6 から直接接続ネイバーに対してアドレス解決を設定するには、グローバル コンフィギュレーション モードで **ipv6 cef optimize neighbor resolution** コマンドを使用します。Cisco Express Forwarding for IPv6 から直接接続ネイバーに対するアドレス解決の最適化を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 cef optimize neighbor resolution
no ipv6 cef optimize neighbor resolution

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

このコマンドを設定しなかった場合、Cisco Express Forwarding for IPv6 は直接接続ネイバーのアドレス解決を最適化しません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 cef optimize neighbor resolution コマンドは、IPv6 固有である点を除いて、**ip cef optimize neighbor resolution** コマンドに非常に似ています。

このコマンドを使用して、直接 Cisco Express Forwarding for IPv6 からネイバーのレイヤ2 アドレス解決をトリガーします。

Examples

次に、Cisco Express Forwarding for IPv6 から直接接続ネイバーに対してアドレス解決を最適化する例を示します。

```
デバイス(config)# ipv6 cef optimize neighbor resolution
```

Related Commands

コマンド	説明
ip cef optimize neighbor resolution	Cisco Express Forwarding for IPv4 からの直接接続ネイバーに対するアドレス解決の最適化を設定します。

ipv6 destination-guard policy

宛先ガードポリシーを定義するには、グローバル コンフィギュレーション モードで **ipv6 destination-guard policy** コマンドを使用します。宛先ガード ポリシーを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 destination-guard policy [policy-name]
no ipv6 destination-guard policy [policy-name]
```

Syntax Description

<i>policy-name</i>	(任意) 宛先ガードポリシーの名前。
--------------------	--------------------

Command Default

宛先ガード ポリシーは定義されません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを実行すると、宛先ガード コンフィギュレーション モードが開始されます。宛先ガードポリシーは、宛先アドレスに基づいてIPv6トラフィックをフィルタ処理し、不明な送信元からのデータトラフィックをブロックするのに使用できます。

Examples

次に、宛先ガードポリシーの名前を定義する例を示します。

```
デバイス(config)#ipv6 destination-guard policy policy1
```

Related Commands

コマンド	説明
show ipv6 destination-guard policy	宛先ガード情報を表示します。

ipv6 dhcp-relay bulk-lease

bulk lease クエリパラメータを設定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp-relay bulk-lease** コマンドを使用します。bulk lease クエリ設定を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp-relay bulk-lease {**data-timeout** *seconds* | **retry** *number*} [**disable**]
no ipv6 dhcp-relay bulk-lease [**disable**]

Syntax Description

data-timeout	(任意) bulk lease クエリ データ転送のタイムアウト。
<i>seconds</i>	(任意) 範囲は 60 ～ 600 秒です。デフォルトは 300 秒です。
retry	(任意) bulk lease クエリの再試行回数を設定します。
<i>number</i>	(任意) 範囲は 0 ～ 5 です。デフォルトは 5 分です。
disable	(任意) DHCPv6 bulk lease クエリ機能を無効にします。

Command Default

bulk lease クエリは、DHCP for IPv6 (DHCPv6) リレー エージェント機能が有効になっている場合は自動的に有効になります。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

データ転送のタイムアウトや bulk lease TCP 接続の試行回数などの bulk lease クエリパラメータを設定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp-relay bulk-lease** コマンドを使用します。

DHCPv6 リレー エージェントが有効になっている場合、DHCPv6 bulk lease クエリ機能は自動的に有効になります。この機能を使用して DHCPv6 bulk lease クエリ機能自体を有効にすることはできません。この機能を無効にするには、**ipv6 dhcp-relay bulk-lease** コマンドと **disable** キーワードを使用します。

Examples

次に、bulk lease クエリ データ転送のタイムアウトを 60 秒に設定する例を示します。

```
デバイス(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

ipv6 dhcp-relay option vpn

DHCP for IPv6 リレーの VRF 認識型機能を有効にするには、グローバル コンフィギュレーション モードで `ipv6 dhcp-relay option vpn` コマンドを使用します。この機能を無効にするには、このコマンドの `no` 形式を使用します。

ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

DHCP for IPv6 リレーの VRF 認識型機能はデバイス上では有効になりません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 dhcp-relay option vpn コマンドは DHCPv6 リレーの VRF 認識型機能をデバイス上でグローバルに有効にすることができます。**ipv6 dhcp relay option vpn** コマンドが指定したインターフェイス上で有効になっている場合は、グローバル **ipv6 dhcp-relay option vpn** コマンドをオーバーライドします。

Examples

次に、DHCPv6 リレーの VRF 認識型機能をデバイス上でグローバルに有効にする例を示します。

```
デバイス(config)# ipv6 dhcp-relay option vpn
```

Related Commands

コマンド	説明
ipv6 dhcp relay option vpn	インターフェイス上で DHCPv6 リレーの VRF 認識型機能を有効にします。

ipv6 dhcp-relay source-interface

メッセージをリレーする場合に送信元として使用するインターフェイスを設定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp-relay source-interface** コマンドを使用します。送信元としてのインターフェイスの使用を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

Syntax Description

<i>interface-type</i> <i>interface-number</i>	(任意) 宛先の出力インターフェイスを指定するインターフェイスのタイプと番号。この引数が設定されている場合、クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。
--	--

Command Default

このサーバ側のインターフェイスのアドレスは、IPv6 リレーの送信元として使用されます。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

設定済みのインターフェイスがシャットダウンされた場合、またはその IPv6 アドレスのすべてが削除された場合、リレーは標準の動作に戻ります。

インターフェイス設定 (インターフェイス コンフィギュレーション モードで **ipv6 dhcp relay source-interface** コマンドを使用) とグローバル設定の両方が設定されている場合は、インターフェイス設定はグローバル設定よりも優先されます。

Examples

次に、リレーの送信元として使用するループバック 0 インターフェイスを設定する例を示します。

```
デバイス(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	インターフェイス上で DHCP for IPv6 サービスを有効にします。

ipv6 dhcp binding track ppp

Dynamic Host Configuration Protocol (DHCP) for IPv6 を設定し、接続が閉じた時点で PPP 接続と関連付けられているバインディングを解放するには、グローバルコンフィギュレーションモードで **ipv6 dhcp binding track ppp** コマンドを使用します。デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

ipv6 dhcp binding track ppp
no ipv6 dhcp binding track ppp

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

PPP 接続を閉じて、その接続に関連付けられている DHCP バインディングは解放されません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 dhcp binding track ppp コマンドは、PPP 接続を閉じたときにその接続と関連付けられているバインディングを自動的に解放するように DHCP for IPv6 を設定します。バインディングを自動的に解放し、十分なリソースを提供することで、後続の新しい登録に対応します。



Note DHCPv6 を使用した IPv6 ブロードバンド展開では、このコマンドを使用して、PPP 仮想インターフェイスに関連付けられているプレフィックスバインディングを解放できるようにする必要があります。これにより、DHCPv6 バインディングが PPP セッションとともに追跡されるようになり、DHCP REBIND が失敗した場合には、クライアントが DHCPv6 ネゴシエーションを再度開始するようになります。

IPv6 用 DHCP サーバのバインディングテーブルエントリに対して、次の処理が自動的に行われます。

- コンフィギュレーションプールからプレフィックスがクライアントに委任されるたびに作成されます。
- クライアントがプレフィックスの委任を更新、再バインディング、または確認すると更新されます。
- クライアントがバインディング内のすべてのプレフィックスを自発的に解放したか、すべてのプレフィックスの有効期限が切れたとき、または管理者がバインディングをクリアしたときに削除されます。

Examples

次に、PPP に関連付けられているプレフィックス バインディングを解放する例を示します。

```
デバイス(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp database

Dynamic Host Configuration Protocol (DHCP) for IPv6 バインディングデータベースを設定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp database** コマンドを使用します。データベースエージェントを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 dhcp database agent [ write-delay seconds ] abort [ timeout seconds ]
no ipv6 dhcp database agent
```

Syntax Description		
agent		フラッシュ、ローカルブートフラッシュ、CompactFlash、NVRAM、FTP、TFTP、または Remote Copy Protocol (RCP) の Uniform Resource Locator。
write-delay seconds		(任意) IPv6 用 DHCP がデータベース更新を送信する頻度 (秒単位)。デフォルトは 300 秒です。最小書き込み遅延は 60 秒です。
timeout seconds		(任意) ルータがデータベース転送を待機する時間 (秒単位)。

Command Default 書き込み遅延のデフォルト値は 300 秒です。タイムアウトのデフォルト値は 300 秒です。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 dhcp database** コマンドは、DHCP for IPv6 バインディングデータベース エージェントのパラメータを指定します。ユーザは複数のデータベース エージェントを設定できます。

バインディングテーブルのエントリは、プレフィックスがコンフィギュレーションプールからクライアントに委任されるたびに自動的に作成され、クライアントがプレフィックス委任を更新、再バインディング、または確認すると更新されます。また、クライアントが自発的にバインディング内のすべてのプレフィックスを解放したとき、すべてのプレフィックスの有効期間が経過したとき、または管理者が **clear ipv6 dhcp binding** コマンドを有効にしたときに削除されます。これらのバインディングは RAM に保持され、**agent** 引数を使用して永続的なストレージに保存できます。これにより、システムのリロード後や電源切断後でも、クライアントに割り当てられたプレフィックスなどの設定に関する情報が失われなくなります。バインディングはテキストレコードとして格納されるため、メンテナンスが容易です。

バインディングデータベースが保存される永続的な各ストレージのことをデータベースエージェントと呼びます。データベースエージェントには、FTP サーバなどのリモート ホストや NVRAM などのローカル ファイル システムがあります。

write-delay キーワードは、DHCP がデータベース更新を送信する頻度を秒単位で指定します。デフォルトでは、IPv6 用 DHCP サーバは、データベース変更の送信前に 300 秒間待機します。

timeout キーワードは、ルータがデータベース転送を待機する時間を秒単位で指定します。無限は 0 秒として定義され、タイムアウト期間を超えた転送はキャンセルされます。デフォルトでは、IPv6 用 DHCP サーバは、データベース転送のキャンセル前に 300 秒間待機します。システムがリロードされる場合、バインディングテーブルが完全に保存されるように転送タイムアウトはありません。

Examples

次に、DHCP for IPv6 バインディング データベース エージェントのパラメータを指定し、バインディング エントリを TFTP に格納する例を示します。

```
デバイス(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

次の例では、DHCP for IPv6 バインディング データベース エージェントのパラメータを指定し、バインディング エントリをブートフラッシュに格納しています。

```
デバイス(config)# ipv6 dhcp database bootflash
```

Related Commands

Command	Description
clear ipv6 dhcp binding	DHCP for IPv6 サーバのバインディング テーブルからクライアントのバインディングを自動的に削除します。
show ipv6 dhcp database	DHCP for IPv6 バインディング データベース エージェントの情報を表示します。

ipv6 dhcp iana-route-add

リレーまたはサーバ上に個別に割り当てられた IPv6 アドレスのルートを追加するには、グローバル コンフィギュレーション モードで **ipv6 dhcp iana-route-add** コマンドを使用します。リレーまたはサーバ上に個別に割り当てられた IPv6 アドレスのルートの追加を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp iana-route-add
no ipv6 dhcp iana-route-add

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトでは、リレーまたはサーバ上に個別に割り当てられた IPv6 アドレスのルートの追加は無効になっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デフォルトでは、**ipv6 dhcp iana-route-add** コマンドは無効になっているため、ルートの追加が必要な場合は有効にする必要があります。アンナンバード インターフェイスを通じてクライアントがリレーまたはサーバに接続されている場合、およびこのコマンドを使用してルートの追加を有効にした場合、Internet Assigned Numbers Authority (IANA) のルートを追加することができます。

Examples 次に、個別に割り当てられている IPv6 アドレスのルートの追加を有効にする例を示します。

```
Device(config)# ipv6 dhcp iana-route-add
```

ipv6 dhcp iapd-route-add

Dynamic Host Configuration Protocol for IPv6（DHCPv6）リレーおよびサーバによって委任プレフィックスに対してルートの追加を有効にするには、グローバルコンフィギュレーションモードで **ipv6 dhcp iapd-route-add** コマンドを使用します。ルートの追加を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp iapd-route-add
no ipv6 dhcp iapd-route-add

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトでは、DHCPv6 リレーおよび DHCPv6 サーバは委任プレフィックスのルートを追加します。

Command Modes グローバル コンフィギュレーション（config）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デフォルトでは、DHCPv6 リレーおよび DHCPv6 サーバは委任プレフィックスのルートを追加します。このコマンドのルート上のプレゼンスは、デバイスがそのデバイスに追加されるという意味ではありません。このコマンドを設定すると、委任プレフィックスのルートは最初のレイヤ 3 リレーおよびサーバ上にも追加されます。

Examples 次に、DHCPv6 リレーおよびサーバを有効にして委任プレフィックスのルートを追加する例を示します。

```
Device(config)# ipv6 dhcp iapd-route-add
```

ipv6 dhcp-ldra

Lightweight DHCPv6 リレーエージェント (LDRA) 機能をアクセスノードで有効にするには、グローバル コンフィギュレーション モードで **ipv6 dhcp-ldra** コマンドを使用します。LDRA 機能を無効にするには、このコマンドの **no** 形式を使用します。

```
ipv6 dhcp-ldra {enable | disable}
no ipv6 dhcp-ldra {enable | disable}
```

Syntax Description

enable アクセスノード上で LDRA 機能を有効にします。

disable アクセスノード上で LDRA 機能を無効にします。

Command Default

デフォルトでは、アクセスノード上で LDRA 機能は有効になっていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

LDRA 機能を VLAN 上またはアクセスノード (デジタル加入者線アクセスマルチプレクサ (DSLAM) またはイーサネットスイッチ) インターフェイスで設定する前に、**ipv6 dhcp-ldra** コマンドを使用して、この機能を有効にする必要があります。

例

次に、LDRA 機能を有効にする例を示します。

```
デバイス(config)# ipv6 dhcp-ldra enable
デバイス(config)# exit
```



Note 上記の例では、デバイスはアクセスノードとなっています。

Related Commands

コマンド	説明
ipv6 dhcp ldra attach-policy	VLAN 上で LDRA 機能を有効にします。
ipv6 dhcp-ldra attach-policy	インターフェイス上で LDRA 機能を有効にします。

ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが ping 動作の一部としてプールアドレスに送信するパケット数を指定するには、グローバルコンフィギュレーションモードで **ipv6 dhcp ping packets** コマンドを使用します。サーバがプールアドレスに ping を送信しないようにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp ping packets *number*
ipv6 dhcp ping packets

Syntax Description

<i>number</i>	アドレスが要求元のクライアントに割り当てられる前に送信された ping パケット数。有効な範囲は 0 ～ 10 です。
---------------	---

Command Default

要求元のクライアントにアドレスが割り当てられるまで、ping パケットは送信されません。

Command Modes

グローバル コンフィギュレーション (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

DHCPv6 サーバは、要求元クライアントにアドレスを割り当てる前にプールアドレスに ping を送信します。ping の応答がない場合、サーバはアドレスが使用されていない可能性が高いと想定し、アドレスを要求元クライアントに割り当てます。

number 引数を 0 に設定すると、DHCPv6 サーバの ping 動作がオフになります。

Examples

次に、ping 試行を停止するまでに DHCPv6 サーバが 4 回試行することを指定する例を示します。

```
デバイス(config)# ipv6 dhcp ping packets 4
```

Related Commands

コマンド	説明
clear ipv6 dhcp conflict	DHCPv6 サーバデータベースからアドレス競合をクリアします。
show ipv6 dhcp conflict	DHCPv6サーバによって検出された、またはクライアントから DECLINE メッセージにより報告されたアドレス競合を表示します。

ipv6 dhcp pool

Dynamic Host Configuration Protocol (DHCP) for IPv6 のサーバ設定情報プールを設定して DHCP for IPv6 プール コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 dhcp pool** コマンドを使用します。DHCP for IPv6 プールを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 dhcp pool poolname
no ipv6 dhcp pool poolname
```

Syntax Description

<i>poolname</i>	ローカルなプレフィックスプールのユーザ定義名。プール名には象徴的な文字列（「Engineering」など）または整数（0 など）を使用できます。
-----------------	--

Command Default

DHCP for IPv6 プールは設定されません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IPv6 用 DHCP サーバ設定情報プールを作成するには、**ipv6 dhcp pool** コマンドを使用します。**ipv6 dhcp pool** コマンドがイネーブルの場合、コンフィギュレーションモードが IPv6 用 DHCP プール コンフィギュレーションモードに変更されます。このモードでは、次のコマンドを使用して、管理者はプレフィックスが委任されるようにプールパラメータを設定し、ドメインネームシステム (DNS) サーバを設定できます。

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] はアドレス割当てにアドレスプレフィックスを設定します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
- **link-address** *IPv6-prefix* はリンクアドレス IPv6 プレフィックスを設定します。着信インターフェイスのアドレスまたはパケット内のリンクアドレスが指定した IPv6 プレフィックスと一致する場合、サーバは設定情報プールを使用します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
- **vendor-specific** *vendor-id* は DHCPv6 ベンダー固有のコンフィギュレーションモードを有効にします。ベンダーの識別番号を指定します。この番号は、ベンダーの IANA プライベートエンタープライズ番号です。指定できる範囲は 1 ~ 4294967295 です。次のコンフィギュレーションコマンドが利用できます。
 - **suboption** *number* はベンダー固有のサブオプション番号を設定します。指定できる範囲は 1 ~ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプションパラメータで定義されている東リに入力できます。



Note **suboption** キーワードの下に **hex** 値を使用すると、入力できるのは 16 進数 (0 ~ f) のみとなります。無効な **hex** 値を入力しても以前の設定は削除されません。

IPv6 用 DHCP 設定情報プールが作成されたら、**ipv6 dhcp server** コマンドを使用して、プールとインターフェイス上のサーバを関連付けます。情報プールを設定しない場合は、**ipv6 dhcp server interface** コンフィギュレーションコマンドを使用して DHCPv6 サーバ関数をインターフェイス上で有効にする必要があります。

DHCPv6 プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6 プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6 アドレス プレフィックスを使用しない場合、プールは設定済みのオプションのみを返します。

link-address コマンドでは、必ずしもアドレスを割り当てなくてもリンクアドレスの照合を行うことができます。プール内の複数のリンクアドレス コンフィギュレーションコマンドを使用して、複数のリレーのプールを照合できます。

アドレスプール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィックスの別のプールについては設定されたオプションだけを返すように設定できます。

Examples

次に、**cisco1** という DHCP for IPv6 設定情報プールを指定して、ルータを DHCP for IPv6 プール コンフィギュレーション モードにする例を示します。

```
デバイス(config)# ipv6 dhcp pool cisco1
デバイス(config-dhcpv6)#
```

次に、IPv6 コンフィギュレーションプール **cisco1** に IPv6 アドレス プレフィックスを設定する例を示します。

```
デバイス(config-dhcpv6)# address prefix 2001:1000::0/64
デバイス(config-dhcpv6)# end
```

次に、3 つのリンクアドレス プレフィックスと IPv6 アドレス プレフィックスを含む **engineering** という名前のプールを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 dhcp pool engineering
デバイス(config-dhcpv6)# link-address 2001:1001::0/64
デバイス(config-dhcpv6)# link-address 2001:1002::0/64
デバイス(config-dhcpv6)# link-address 2001:2000::0/48
デバイス(config-dhcpv6)# address prefix 2001:1003::0/64
デバイス(config-dhcpv6)# end
```

次に、ベンダー固有オプションを含む **350** という名前のプールを設定する例を示します。

```
デバイス# configure terminal  
デバイス(config)# ipv6 dhcp pool 350  
デバイス(config-dhcpv6)# vendor-specific 9  
デバイス(config-dhcpv6-vs)# suboption 1 address 1000:235D::1デバイス(config-dhcpv6-vs)# suboption  
2 ascii "IP-Phone"  
デバイス(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	インターフェイス上で DHCP for IPv6 サービスを有効にします。
show ipv6 dhcp pool	DHCP for IPv6 コンフィギュレーションプール情報を表示します。

ipv6 dhcp server vrf enable

DHCP for IPv6 サーバの VRF 認識型機能を有効にするには、グローバル コンフィギュレーション モードで **ipv6 dhcp server vrf enable** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

```
ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable
```

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default DHCPv6 サーバの VRF 認識型機能は有効になりません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 dhcp server option vpn** コマンドは DHCPv6 サーバの VRF 認識型機能をデバイス上でグローバルに有効にすることができます。

Examples

次に、DHCPv6 サーバの VRF 認識型機能をデバイス上でグローバルに有効にする例を示します。

```
デバイス(config)# ipv6 dhcp server option vpn
```

ipv6 flow monitor

このコマンドは、着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。

以前に作成したフローモニタをアクティブにするには、**ipv6 flow monitor** コマンドを使用します。フローモニタを非アクティブにするには、このコマンドの **no** 形式を使用します。

```
ipv6 flow monitor ipv6-monitor-name [sampler ipv6-sampler-name] {input | output}
no ipv6 flow monitor ipv6-monitor-name [sampler ipv6-sampler-name] {input | output}
```

Syntax Description	
<i>ipv6-monitor-name</i>	着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。
sampler <i>ipv6-sampler-name</i>	フロー モニタ サンプラーを適用します。
input	入力トラフィックにフロー モニタを適用します。
output	出力トラフィックにフロー モニタを適用します。

Command Default IPv6 フロー モニタは、インターフェイスに割り当てられるまでアクティブになりません。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ポート チャネル インターフェイスには NetFlow モニタを接続できません。サービス モジュールの両方のインターフェイスが EtherChannel の一部である場合、両方の物理インターフェイスにモニタを接続する必要があります。

次に、フロー モニタをインターフェイスに適用する例を示します。

```
デバイス(config)# interface gigabitethernet 1/1/2
デバイス(config-if)# ip flow monitor FLOW-MONITOR-1 input
デバイス(config-if)# ip flow monitor FLOW-MONITOR-2 output
デバイス(config-if)# end
```

ipv6 general-prefix

IPv6 の汎用プレフィックスを定義するには、グローバル コンフィギュレーション モードで **ipv6 general-prefix** コマンドを使用します。IPv6 の汎用プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 general-prefix prefix-name {ipv6-prefix/prefix-length | 6to4 interface-type interface-number | 6rd interface-type interface-number}
no ipv6 general-prefix prefix-name
```

Syntax Description

<i>prefix-name</i>	プレフィックスに割り当てられている名前。
<i>ipv6-prefix</i>	汎用プレフィックスに割り当てられている IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。 汎用プレフィックスを手動で定義する場合は、 <i>ipv6-prefix</i> 引数と <i>/prefix-length</i> 引数の両方を指定します。
<i>/ prefix-length</i>	IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 汎用プレフィックスを手動で定義する場合は、 <i>ipv6-prefix</i> 引数と <i>/prefix-length</i> 引数の両方を指定します。
6to4	6to4 トンネリングに使用するインターフェイスに基づいて汎用プレフィックスを設定できます。 6to4 インターフェイスに基づいて汎用プレフィックスを定義する場合は、 6to4 キーワードと <i>interface-type interface-number</i> 引数を指定します。
<i>interface-type interface-number</i>	インターフェイスのタイプと番号。詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。 6to4 インターフェイスに基づいて汎用プレフィックスを定義する場合は、 6to4 キーワードと <i>interface-type interface-number</i> 引数を指定します。
6rd	IPv6 高速展開 (6RD) トンネリングに使用するインターフェイスからキャプチャした汎用プレフィックスを設定できます。

Command Default

汎用プレフィックスは定義されません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 general-prefix コマンドを使用して IPv6 汎用プレフィックスを定義します。

汎用プレフィックスには、短いプレフィックスが保持されます。このプレフィックスに基づいて、より長く詳細な複数のプレフィックスを定義できます。汎用プレフィックスが変更されると、そのプレフィックスに基づくより詳細なプレフィックスもすべて変更されます。この機能により、ネットワーク リナンバリングが大幅に簡略化され、自動化されたプレフィックス定義が可能になります。

汎用プレフィックスに基づくより詳細なプレフィックスは、インターフェイスに IPv6 を設定する場合に使用できます。

6to4 トンネリングに使用するインターフェイスに基づく汎用プレフィックスを定義する場合、汎用プレフィックスは 2002:a.b.c.d::/48 の形式になります。「a.b.c.d」は、参照されるインターフェイスの IPv4 アドレスです。

Examples

次に、my-prefix という IPv6 汎用プレフィックスを手動で定義する例を示します。

```
デバイス(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

次に、my-prefix という IPv6 汎用プレフィックスを 6to4 インターフェイスに基づいて定義する例を示します。

```
デバイス(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

Related Commands

Command	Description
show ipv6 general-prefix	IPv6 アドレスの汎用プレフィックスに関する情報を表示します。

ipv6 local policy route-map

ローカル ポリシーベース ルーティング (PBR) を IPv6 パケットに有効にするには、グローバル コンフィギュレーション モードで **ipv6 local policy route-map** コマンドを使用します。IPv6 パケットのローカル ポリシーベース ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 local policy route-map *route-map-name*
no ipv6 local policy route-map *route-map-name*

Syntax Description

<i>route-map-name</i>	ローカル IPv6 PBR に使用するルート マップの名前。この名前は、 route-map コマンドで指定した <i>route-map-name</i> 値に一致している必要があります。
-----------------------	--

Command Default

IPv6 パケットはポリシー ルーティングされません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

通常、ルータから発信されるパケットはポリシー ルーティングされません。ただし、このようなパケットをポリシー ルーティングするには、**ipv6 local policy route-map** コマンドを使用します。明白な最短パス以外のルートを取るルータでパケットを発信する場合は、ローカル PBR を有効にすることができます。

ipv6 local policy route-map コマンドは、ローカル PBR に使用するルートマップを識別します。**route-map** コマンドのそれぞれには、それらに関連付けられた **match** コマンドと **set** コマンドのリストが備わっています。**match** コマンドは一致基準を指定します。この基準は、パケットをポリシー ルーティングする条件となります。**set** コマンドは **match** コマンドによって適用された基準が満たされている場合に実行される特定のポリシー ルーティング アクションである **set** アクションを指定します。**no ipv6 local policy route-map** コマンドは、ルートマップへの参照を削除し、ローカル ポリシー ルーティングを無効にします。

Examples

次に、宛先 IPv6 アドレスがアクセス リスト **pbr-src-90** で許可されているアドレスに一致するパケットが IPv6 アドレス **2001:DB8::1** のルータに送信される例を示します。

```
ipv6 access-list src-90
 permit ipv6 host 2001::90 2001:1000::/64
route-map pbr-src-90 permit 10
 match ipv6 address src-90
  set ipv6 next-hop 2001:DB8::1
ipv6 local policy route-map pbr-src-90
```

Related Commands	コマンド	説明
	ipv6 policy route-map	インターフェイス上に IPv6 PBR を設定します。
	match ipv6 address	IPv6 の PBR でパケットの照合に使用する IPv6 アクセス リストを指定します。
	match length	パケットのレベル 3 長に基づいてポリシー ルーティングを実行します。
	route-map (IP)	あるルーティングプロトコルから別のルーティングプロトコルヘルトを再配布する条件を定義するか、ポリシー ルーティングをイネーブルにします。
	set default interface	ポリシー ルーティングのルートマップの match 句を満たし、宛先までの明示的なルートを持たないパケットを出力するデフォルトのインターフェイスを指定します。
	set interface	ポリシー ルーティングのルートマップの match 句を満たしたパケットを出力するデフォルトのインターフェイスを指定します。
	set ipv6 default next-hop	一致パケットが転送されるデフォルトの IPv6 ネクスト ホップを指定します。
	set ipv6 next-hop (PBR)	ポリシー ルーティングのルート マップの match 句を満たした IPv6 パケットの出力先を指定します。
	set ipv6 precedence	IPv6 パケット ヘッダーのプリファレンス値を設定します。

ipv6 local pool

ローカル IPv6 プレフィックス プールを設定するには、プレフィックスにプール名を指定した `ipv6 local pool` コンフィギュレーション コマンドを使用します。プールを無効にするには、このコマンドの `no` 形式を使用します。

```
ipv6 local pool poolname prefix/prefix-length assigned-length [shared] [cache-size size]
no ipv6 local pool poolname
```

Syntax Description

<i>poolname</i>	ローカルなプレフィックス プールのユーザ定義名。
<i>prefix</i>	プールに割り当てられている IPv6 プレフィックス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>/ prefix-length</i>	プールに割り当てられている IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。
<i>assigned-length</i>	プールからユーザに割り当てられがプレフィックスの長さ（ビット単位）。 <i>assigned-length</i> 引数の値は、 <i>/prefix-length</i> 引数の値未満であってはなりません。
shared	（任意）プールが共有プールであることを示します。
cache-size size	（任意）キャッシュのサイズを指定します。

Command Default

プールは設定されません。

Command Modes

グローバル コンフィギュレーション（global）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

すべてのプール名が固有である必要があります。

IPv6 プレフィックス プールには IPv4 アドレス プールに類似している関数があります。IPv4 とは対照的に、割り当てられているアドレスのブロック（アドレスプレフィックス）は単一アドレスではありません。

プレフィックス プールの重複は許可されていません。

プールが設定されたあとは、プールを変更できません。設定を変更するには、プールを削除して作成し直す必要があります。すでに割り当てられていたすべてのプレフィックスが解放されます。

Examples

次に、IPv6 プレフィックス プールを作成する例を示します。

```
デバイス(config)# ipv6 local pool pool1 2001:0DB8::/29 64
デバイス(config)# end
デバイス# show ipv6 local pool
Pool Prefix Free In use
pool1 2001:0DB8::/29 65516 20
```

Related Commands

コマンド	説明
debug ipv6 pool	IPv6 プールのデバッグを有効にします。
peer default ipv6 address pool	クライアントプレフィックスを PPP リンクに割り当てるプールを指定します。
prefix-delegation pool	プレフィックスを IPv6 クライアントの DHCP に委任する名前付きの IPv6 ローカルプレフィックスプールを指定します。
show ipv6 local pool	定義済みの IPv6 アドレスプールに関する情報を表示します。

ipv6 mld snooping (グローバル)

マルチキャストリスナー検出バージョン2 (MLDv2) プロトコルスヌーピングをグローバルに有効にするには、グローバル コンフィギュレーション モードで **ipv6 mld snooping** コマンドを使用します。MLDv2 スヌーピングをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping
no ipv6 mld snooping

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default このコマンドは有効です。

Command Modes グローバル コンフィギュレーション (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが Supervisor Engine 720 に導入されました。

Usage Guidelines MLDv2 スヌーピングは、ポリシー フィーチャ カード 3 (PFC3) の何らかのバージョンが搭載された Supervisor Engine 720 でサポートされています。

MLDv2 スヌーピングを使用するには、IPv6 マルチキャストルーティング用のサブネットでレイヤ3 インターフェイスを設定するか、またはサブネットで MLDv2 スヌーピング クエリアを有効にします。

Examples

次に、MLDv2 スヌーピングをグローバルにイネーブルにする例を示します。

```
デバイス(config)# ipv6 mld snooping
```

コマンド	説明
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

ipv6 mld ssm-map enable

送信元特定マルチキャスト（SSM）マッピング機能を設定済みのSSM範囲内にあるグループに有効にするには、グローバル コンフィギュレーション モードで **ipv6 mld ssm-map enable** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

```
ipv6 mld [vrf vrf-name] ssm-map enable
no ipv6 mld [vrf vrf-name] ssm-map enable
```

Syntax Description	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
---------------------------	----------------------------	--

Command Default SSM マッピング機能は有効になりません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 mld ssm-map enable** コマンドは、設定済みのSSM範囲内にあるグループにSSMマッピング機能を有効にします。**ipv6 mld ssm-map enable** コマンドを使用すると、SSMマッピングはデフォルトでドメインネームシステム (DNS) を使用します。

SSMマッピングは、受信したマルチキャストリスナー検出 (MLD) バージョン1またはMLDバージョン2のメンバーシップレポートにのみ適用されます。

Examples

次に、SSMマッピング機能を有効にする例を示します。

```
デバイス(config)# ipv6 mld ssm-map enable
```

Related Commands	コマンド	説明
	debug ipv6 mld ssm-map	SSMマッピングのデバッグメッセージを表示します。
	ipv6 mld ssm-map query dns	DNSベースのSSMマッピングを有効にします。
	ipv6 mld ssm-map static	スタティックSSMマッピングを設定します。
	show ipv6 mld ssm-map	SSMマッピング情報を表示します。

ipv6 mld state-limit

マルチキャストリスナー検出（MLD）の状態数をグローバルに制限するには、グローバル コンフィギュレーション モードで **ipv6 mld state-limit** コマンドを使用します。設定済みの MLD 状態の制限を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*
no ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*

Syntax Description

vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
<i>number</i>	ルータで許可される MLD の状態の最大数。有効な範囲は 1 ～ 64000 です。

Command Default

MLD 制限のデフォルト数は設定されません。このコマンドの設定時に、ルータ上でグローバルに許可する最大 MLD 状態数を設定する必要があります。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

MLD メンバーシップレポートの結果の MLD 状態数の制限をグローバルに設定するには、**ipv6 mld state-limit** コマンドを使用します。設定した制限を超過した後に送信されたメンバーシップレポートは MLD キャッシュには入力されず、超過した分のメンバーシップレポートのトラフィックは転送されません。

インターフェイスごとの MLD 状態の制限を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mld limit** コマンドを使用します。

インターフェイスごとの制限およびシステムごとの制限はそれぞれ個別に機能し、設定済みのさまざまな制限を適用できます。メンバーシップの状態は、インターフェイスごとの制限またはグローバル制限のいずれかを超過した場合は無視されます。

Examples

次に、ルータ上の MLD 状態数を 300 に制限する例を示します。

```
デバイス(config)# ipv6 mld state-limit 300
```

Related Commands

コマンド	説明
ipv6 mld access-group	IPv6 マルチキャスト受信者アクセス制御のパフォーマンスを有効にします。

コマンド	説明
ipv6 mld limit	MLD メンバシップ状態の結果の MLD 状態数をインターフェイスごとに制限します。

ipv6 multicast-routing

Protocol Independent Multicast (PIM) とマルチキャストリスナー検出 (MLD) を使用してルータの IPv6 対応のすべてのインターフェイス上でマルチキャストルーティングを有効にし、マルチキャスト転送を有効にするには、グローバル コンフィギュレーション モードで **ipv6 multicast-routing** コマンドを使用します。マルチキャストルーティングと転送を停止するには、このコマンドの **no** 形式を使用します。

```
ipv6 multicast-routing [vrf vrf-name ]
no ipv6 multicast-routing
```

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
----------------------------	--

Command Default

マルチキャストルーティングは無効になりません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

マルチキャスト転送を有効にするには、**ipv6 multicast-routing** コマンドを使用します。このコマンドは、設定するルータの IPv6 対応のすべてのインターフェイス上で Protocol Independent Multicast (PIM) とマルチキャストリスナー検出 (MLD) も有効にします。

マルチキャストを有効にする前に個々のインターフェイスを設定し、必要に応じてそれらのインターフェイス上での PIM および MLD のプロトコル処理を明示的に無効にすることができます。IPv6 PIM または MLD のルータ側の処理を無効にするには、それぞれ **no ipv6 pim** コマンドまたは **no ipv6 mld router** コマンドを使用します。

Examples

次に、マルチキャストルーティングを有効にし、すべてのインターフェイス上で PIM と MLD をオンにする例を示します。

```
デバイス(config)# ipv6 multicast-routing
```

Related Commands

コマンド	説明
ipv6 pim rp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
no ipv6 pim	指定したインターフェイスで IPv6 PIM をオフにします。
no ipv6 mld router	指定したインターフェイスで MLD ルータ側処理をディセーブルにします。

ipv6 multicast group-range

すべてのインターフェイス上で未承認グループまたはチャンネルのマルチキャストプロトコルのアクションとトラフィック転送を無効にするには、グローバル コンフィギュレーション モードで **ipv6 multicast group-range** コマンドを使用します。コマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
ipv6 multicast [vrf vrf-name ] group-range [access-list-name]
no ipv6 multicast [vrf vrf-name ] group-range [access-list-name]
```

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>access-list-name</i>	(任意) トラフィックをルータに送信できる認証済みのサブスクリバグループと承認済みのチャンネルを含んでいるアクセス リストの名前。

Command Default

指定したアクセス リストで許可されているグループとチャンネルに対してマルチキャストが有効になり、指定したアクセス リストで拒否されているグループとチャンネルのマルチキャストは無効になります。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 multicast group-range コマンドは、IPv6 マルチキャスト エッジルーティングにアクセス制御メカニズムを提供します。*access-list-name* 引数で指定されたアクセス リストは、許可または拒否されるマルチキャストグループまたはチャンネルを指定します。拒否されたグループまたはチャンネルについては、ルータがプロトコルトラフィックとアクションを無視し(たとえば、マルチキャストリスナー検出 (MLD) 状態が作成されない、マルチキャストルータの状態が作成されない、Protocol Independent Multicast (PIM) の join は転送されないなど)、システム内のすべてのインターフェイスでデータトラフィックをドロップします。そのため、拒否されたグループまたはチャンネルのマルチキャストは無効になります。

ipv6 multicast group-range グローバル コンフィギュレーション コマンドを使用すると、システム内のすべてのインターフェイス上で MLD アクセス制御コマンドとマルチキャスト境界作成コマンドを設定することになります。ただし、**ipv6 multicast group-range** コマンドは、次のインターフェイス コンフィギュレーション コマンドを使用することで、選択したインターフェイス上でオーバーライドできます。

- **ipv6 mld access-group** *access-list-name*
- **ipv6 multicast boundary scope** *scope-value*

no ipv6 multicast group-range コマンドはルータをデフォルト設定に戻すため、既存のマルチキャスト展開は破損しません。

Examples

次に、list2 というアクセス リストによって拒否されたグループまたはチャンネルのマルチキャストをルータが確実に無効にする例を示します。

```
デバイス(config)# ipv6 multicast group-range list2
```

次に、前出の例のコマンドが int2 によって指定されたインターフェイス上でオーバーライドされる例を示します。

```
デバイス(config)# interface int2
```

```
デバイス(config-if)# ipv6 mld access-group int-list2
```

int2 では、int-list2 によって許可されたグループまたはチャンネルに MLD の状態が作成されますが、int-list2 によって拒否されたグループまたはチャンネルには作成されません。その他のすべてのインターフェイスでは、list2 というアクセス リストがアクセス制御に使用されます。

この例では、すべて、またはほとんどのマルチキャストグループまたはチャンネルを拒否するように list2 を指定することができ、int-list2 はインターフェイス int2 に対してのみ、承認済みのグループまたはチャンネルを許可するように指定できます。

Related Commands

Command	Description
ipv6 mld access-group	IPv6 マルチキャスト受信者アクセス制御を実行します。
ipv6 multicast boundary scope	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。

ipv6 multicast pim-passive-enable

IPv6 ルータ上で Protocol Independent Multicast (PIM) パッシブ機能を有効にするには、グローバル コンフィギュレーションモードで **ipv6 multicast pim-passive-enable** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 multicast pim-passive-enable
no ipv6 multicast pim-passive-enable

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default PIM パッシブ モードはルータ上で有効になりません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ルータ上で IPv6 PIM パッシブモードを設定するには、**ipv6 multicast pim-passive-enable** コマンドを使用します。PIM パッシブモードがグローバルに設定されたら、インターフェイス コンフィギュレーションモードで **ipv6 pim passive** コマンドを使用して特定のインターフェイス上で PIM パッシブモードを設定します。

Examples 次に、ルータ上で IPv6 PIM パッシブ モードを設定する例を示します。

```
デバイス(config)# ipv6 multicast pim-passive-enable
```

Related Commands	コマンド	説明
	ipv6 pim passive	特定のインターフェイス上で PIM パッシブモードを設定します。

ipv6 nd cache expire

IPv6 ネイバー探索のキャッシュエントリの有効期限が切れるまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd cache expire** コマンドを使用します。この設定を削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]
no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

Syntax Description

expire-time-in-seconds

時間の範囲は 1 ～ 65,536 秒です。デフォルトは 14,400 秒、です。

refresh

(任意) ネイバー探索キャッシュエントリを自動的に更新し

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

デフォルトでは、14,400 秒間、つまり 4 時間にわたって STALE 状態が続いた場合は、ネイバー探索キャッシュエントリの有効期限が切れて削除されます。 **ipv6 nd cache expire** コマンドを使用すると、有効期限を変更したり、エントリが削除される前に期限切れのエントリの自動更新をトリガーすることができます。

refresh キーワードを使用すると、ネイバー探索キャッシュエントリが自動更新されます。エントリは DELAY 状態に移行し、ネイバー到達不能検出プロセスが実行され、5 秒後にエントリは DELAY 状態から PROBE 状態に遷移します。エントリが PROBE 状態に到達すると、ネイバー送信要求が送信され、設定に従って再送信されます。

Examples

次に、ネイバー探索キャッシュエントリが 7,200 秒 (2 時間) で期限が切れるように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

Related Commands

コマンド	説明
ipv6 nd na glean	非送信要求ネイバーアドバタイズメントからエントリを収集するネイバー探索を設定します。
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。

コマンド	説明
show ipv6 interface	IPv6用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ipv6 nd cache interface-limit (global)

デバイス上のすべてのインターフェイスにネイバー探索のキャッシュ制限を設定するには、グローバル コンフィギュレーション モードで **ipv6 nd cache interface-limit** コマンドを使用します。デバイス上のすべてのインターフェイスからネイバー探索を削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd cache interface-limit *size* [*log rate*]
no ipv6 nd cache interface-limit *size* [*log rate*]

Syntax Description	
<i>size</i>	キャッシュ サイズ。
log rate	(任意) 調節可能なロギング レート (秒単位)。有効な値は 0 と 1 です。

Command Default デバイスのデフォルトのロギング レートは 1 秒あたり 1 エントリです。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines グローバル コンフィギュレーション モードで **ipv6 nd cache interface-limit** コマンドを実行すると、デバイス上のすべてのインターフェイスに共通のインターフェイスごとのキャッシュ サイズを適用します。

このコマンドの **no** 形式またはデフォルトの形式を発行すると、グローバル コンフィギュレーション モードを使用して設定したデバイス上のすべてのインターフェイスからネイバー探索制限が削除されます。インターフェイス コンフィギュレーション モードで **ipv6 nd cache interface-limit** コマンドを使用して設定したインターフェイスのネイバー探索制限は削除されません。

デバイスのデフォルト (および最大) のロギング レートは 1 秒あたり 1 エントリです。

Examples

次に、デバイス上のすべてのインターフェイスに共通のインターフェイスごとのキャッシュ サイズ制限を 4 秒に設定する例を示します。

```
デバイス(config)# ipv6 nd cache interface-limit 4
```

Related Commands	コマンド	説明
	ipv6 nd cache interface-limit (interface)	デバイス上の指定したインターフェイスにネイバー探索 キャッシュ 制限を設定します。

ipv6 nd host mode strict

conformant または strict IPv6 ホストモードを有効にするには、グローバル コンフィギュレーション モードで **ipv6 nd host mode strict** コマンドを使用します。conformant または loose IPv6 ホストモードを再度有効にするには、このコマンドの **no** 形式を使用します。

ipv6 nd host mode strict

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

nonconformant、または loose IPv6 ホストモードが有効になります。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デフォルトの IPv6 ホストモードタイプは loose または nonconformant です。IPv6 strict または conformant のホストモードを有効にするには、**ipv6 nd host mode strict** コマンドを使用します。2 つの IPv6 ホストモード間で変更を行うには、このコマンドの **no** 形式を使用します。

ipv6 nd host mode strict コマンドは、IPv6 ホストモード動作タイプを選択し、インターフェイス コンフィギュレーションモードに移行します。ただし、**ipv6 nd host mode strict** コマンドは、**ipv6 unicast-routing** コマンドを使用して設定した IPv6 ルーティングがある場合は無視されます。この状況では、デフォルトの IPv6 ホストモードタイプの loose が使用されます。

Examples

次に、strict IPv6 ホストとしてデバイスを設定し、イーサネット インターフェイス 0/0 で IPv6 アドレスの自動設定を有効にする例を示します。

```
デバイス(config)# ipv6 nd host mode strict
デバイス(config-if)# interface ethernet0/0
デバイス(config-if)# ipv6 address autoconfig
```

次に、strict IPv6 ホストとしてデバイスを設定し、イーサネット インターフェイス 0/0 で 静的 IPv6 アドレスを設定する例を示します。

```
デバイス(config)# ipv6 nd host mode strict
デバイス(config-if)# interface ethernet0/0
デバイス(config-if)# ipv6 address 2001::1/64
```

Related Commands

コマンド	説明
ipv6 unicast-routing	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

ipv6 nd na glean

非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd na glean** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 nd na glean
no ipv6 nd na glean

Command Modes インターフェイス コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 重複アドレス検出 (DAD) が正常に完了すると、IPv6 ノードからマルチキャスト非送信要求ネイバーアドバタイズメントパケットが発行されることがあります。デフォルトでは、これらの非送信要求ネイバーアドバタイズメントパケットは他の IPv6 ノードから無視されます。**ipv6 nd na glean** コマンドは、非送信要求ネイバーアドバタイズメントパケットの受信時にルータでネイバーアドバタイズメントエントリを作成するように設定します (これらのエントリがまだ存在せず、ネイバーアドバタイズメントにリンク層アドレスオプションがある場合)。このコマンドを使用すると、データトラフィックをネイバーと交換する前に、デバイスのネイバーアドバタイズメント キャッシュにネイバーのエントリを読み込むことができます。

Examples

次に、非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

Related Commands

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索キャッシュエントリの期限が切れるまでの時間を設定します。
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
show ipv6 interface	IPv6用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ipv6 nd ns-interval

インターフェイスでIPv6 ネイバー送信要求（NS）メッセージが再送信される時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ns-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

Syntax Description	<i>milliseconds</i>	アドレス解決のためのIPv6 ネイバー探索伝送の間隔。許容範囲は1,000～3,600,000 ミリ秒です。
---------------------------	---------------------	--

Command Default 0 ミリ秒（未指定）の場合、ルータ アドバタイズメントでアドバタイズされます。値 1000 は、ルータ自体のネイバー探索アクティビティに使用されます。

Command Modes インターフェイス コンフィギュレーション（config-if）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デフォルトでは、**ipv6 nd ns-interval** コマンドはアドレス解決と重複アドレス検出（DAD）の両方の NS 再送信間隔を変更します。DAD に別の NS の再送信間隔を指定するには、**ipv6 nd dad time** コマンドを使用します。

この値は、このインターフェイスから送信されるすべてのIPv6 ルータアドバタイズメントに含まれます。通常のIPv6 操作には、短すぎる間隔はお勧めできません。デフォルト以外の値が設定されている場合、設定時間は、ルータ自体により、アドバタイズおよび使用されます。

Examples

次に、イーサネットインターフェイス 0/0 のIPv6 ネイバー送信要求メッセージの送信間隔を 9,000 ミリ秒に設定する例を示します。

```
デバイス(config)# interface ethernet 0/0
デバイス(config-if)# ipv6 nd ns-interval 9000
```

Related Commands	コマンド	説明
	ipv6 nd dad time	アドレス解決のための NS 再送信間隔とは別に DAD の NS 再送信間隔を設定します。
	show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd nud retry

ネイバー到達不能検出プロセスでネイバー送信要求を再送信する回数を設定するには、インターフェイスコンフィギュレーションモードで **ipv6 nd nud retry** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 nd nud retry *base interval max-attempts {final-wait-time}*
no ipv6 nd nud retry *base interval max-attempts {final-wait-time}*

Syntax Description

<i>base</i>	ネイバー到達不能検出プロセスのベース値。 間隔
<i>max-attempts</i>	再試行の最大回数（ベース値に依存）。 有効な範囲は 1000 ～ 32000 です。
<i>final-wait-time</i>	再試行の最大回数（ベース値に依存）。 有効な範囲は 1 ～ 128 です。
	最後のプローブの待機時間（ミリ秒）。 有効な範囲は 1000 ～ 32000 です。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ネイバーのネイバー検出エントリを再度解決するためにデバイスでネイバー到達不能検出を実行する際、ネイバー送信要求パケットが1秒間隔で3回送信されます。スパニングツリーイベント、トラフィックの多いイベント、エンドホストのリロードなどの特定の状況においては、ネイバー送信要求が1秒間隔で3回送信されても十分でない場合があります。このような状況でネイバーキャッシュを維持するには、**ipv6 nd nud retry** コマンドを使用してネイバー送信要求の再送信の指数タイマーを設定します。

再試行の最大回数は、*max-attempts* 引数を使用して設定されます。再送信間隔は、次の式で計算されます。

$$tm^n$$

各値は次のとおりです。

- t = 時間間隔
- m = ベース (1、2、または 3)
- n = 現在のネイバー送信要求番号 (最初のネイバー送信要求が 0)

したがって、**ipv6 nd nud retry 3 1000 5** コマンドは、1、3、9、27、81 秒の間隔で再送信します。最終待機時間が設定されていない場合、エントリは 243 秒後に削除されます。

ipv6 nd nud retry コマンドはネイバー到達不能検出プロセスの再送信レートにのみ影響し、最初の解決には影響しません。最初の解決では、デフォルトに基づいてネイバー送信要求パケットが 1 秒間隔で 3 回送信されます。

Examples

次に、1 秒の固定間隔で 3 回再送信するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

次に、再送信間隔を 1、2、4、8 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

次に、再送信間隔を 1、3、9、27、81 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

Related Commands

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索 (ND) キャッシュエントリの期限が切れるまでの時間を設定します。
ipv6 nd na glean	非送信要求ネイバーアドバタイズメントからエントリを収集するネイバー探索を設定します。
show ipv6 interface	IPv6用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ipv6 nd reachable-time

何らかの到達可能性確認イベントが発生してからリモート IPv6 ノードが到達可能と見なされるまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *milliseconds*
no ipv6 nd reachable-time

Syntax Description

<i>milliseconds</i>	リモート IPv6 ノードが到達可能であると見なされる時間（ミリ秒単位）。
---------------------	---------------------------------------

Command Default

0 ミリ秒（未指定）の場合、ルータ アドバタイズメントでアドバタイズされます。値 30000（30 秒）は、ルータ自体のネイバー探索アクティビティに使用されます。

Command Modes

インターフェイス コンフィギュレーション（config-if）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

設定時間により、ルータは、利用不可隣接を検出できます。設定時間を短くすると、ルータは、より速く利用不可隣接を検出できます。ただし、設定時間を短くすると、すべての IPv6 ネットワーク デバイスで消費される IPv6 ネットワーク 帯域幅および処理リソースが多くなります。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

設定時間は、インターフェイスから送信されるすべてのルータ アドバタイズメントに含まれるため、同じリンクのノードは同じ時間値を共有します。値に 0 を設定すると、設定時間がこのルータで指定されていないことを示します。

Examples

次に、イーサネット インターフェイス 0/0 に 1,700,000 ミリ秒の IPv6 到達可能時間を設定する例を示します。

```
デバイス(config)# interface ethernet 0/0
デバイス(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd resolution data limit

ネイバー探索保留中のキュー登録データパケットの数を設定するには、グローバル コンフィギュレーション モードで **ipv6 nd resolution data limit** コマンドを使用します。

ipv6 nd resolution data limit *number-of-packets*
no ipv6 nd resolution data limit *number-of-packets*

Syntax Description	<i>number-of-packets</i> キュー登録データ パケット数。範囲は 16 ～ 2048 パケットです。
---------------------------	---

Command Default キュー制限は 16 パケットです。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 nd resolution data limit** コマンドを使用すると、顧客はネイバー探索解決保留中のパケットのキュー登録数を設定できます。IPv6 ネイバー探索は、未解決の宛先の解決を開始するデータ パケットをキューに登録します。ネイバー探索は、宛先ごとに 1 つのパケットのみをキューに登録します。また、ネイバー探索はキューに登録されるパケットの数にグローバル (ルータごとの) 制限も適用します。グローバル キュー制限に到達すると、未解決の宛先へのそれ以降のパケットが破棄されます。最小値 (およびデフォルト値) は 16 パケットで、最大値は 2048 です。

ほとんどの場合は、ネイバー探索解決保留中のキュー登録パケットのデフォルト値の 16 で十分です。ただし、極めて多くのネイバーとの通信をほぼ同時に開始する必要があるルータの高拡張性シナリオでは、この値では不十分な場合があります。そのため、一部のネイバーに送信された最初のパケットが失われる可能性があります。ほとんどの場合、最初のパケットは再送信されるため、通常は、最初のパケットの損失について心配する必要はありません (未解決の宛先への最初のパケットのドロップは IPv4 では正常な動作です)。ただし、最初のパケットの損失が問題となる大規模設定もあります。このような場合は **ipv6 nd resolution data limit** コマンドを使用し、未解決パケットキューのサイズを拡大することで最初のパケット損失を防ぎます。

Examples

次に、解決待機中に保持されるデータ パケットのグローバル数を 32 に設定する例を示します。

```
デバイス(config)# ipv6 nd resolution data limit 32
```

ipv6 nd route-owner

ネイバー探索で学習したルートを「ND」ステータスでルーティングテーブルに挿入し、ND 自動設定動作を有効にするには、**ipv6 nd route-owner** コマンドを使用します。ルーティングテーブルからこの情報を削除するには、このコマンドの **no** 形式を使用します。

ipv6 ndroute-owner

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default ネイバー探索で学習したルートのステータスは「Static」です。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 nd route-owner** コマンドはネイバー探索で学習したルートを「Static」または「Connected」ではなく、「ND」のステータスでルーティングテーブルに挿入します。

また、このグローバルコマンドはインターフェイス コンフィギュレーション モードで **ipv6 nd autoconfig default** コマンドまたは **ipv6 nd autoconfig prefix** コマンドも使用できるようにします。**ipv6 nd route-owner** コマンドを発行しないと、**ipv6 nd autoconfig default** コマンドと **ipv6 nd autoconfig prefix** コマンドはルータには承認されますが、機能しません。

Examples デバイス(config)# **ipv6 nd route-owner**

Related Commands	コマンド	説明
	ipv6 nd autoconfig default	ネイバー探索によって、ネイバー探索で取得されたデフォルトルータにデフォルト ルートをインストールできるようにします。
	ipv6 nd autoconfig prefix	ネイバー探索を使用して、インターフェイスで受信した RA から有効なすべてのオンリンク プレフィックスをインストールします。

ipv6 neighbor

IPv6 ネイバー探索キャッシュにスタティックエントリを設定するには、グローバルコンフィギュレーションモードで **ipv6 neighbor** コマンドを使用します。IPv6 ネイバー探索キャッシュからスタティック IPv6 エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 neighbor *ipv6-address interface-type interface-number hardware-address*
no ipv6 neighbor *ipv6-address interface-type interface-number*

Syntax Description		
<i>ipv6-address</i>	ローカルデータリンク アドレスに対応する IPv6 アドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。	
<i>interface-type</i>	指定されたインターフェイス タイプ。サポートされているインターフェイス タイプについては、疑問符 (?) オンラインヘルプ機能を使用してください。	
<i>interface-number</i>	指定されたインターフェイス番号。	
<i>hardware-address</i>	ローカルデータリンク アドレス (48 ビットアドレス)。	

Command Default スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 neighbor** コマンドは **arp** (グローバル) コマンドに類似しています。

指定された IPv6 アドレスのエントリが (IPv6 ネイバー探索プロセスを通して学習された) ネイバー探索キャッシュ内にすでに存在する場合、そのエントリは自動的に静的エントリに変換されます。

show ipv6 neighbors コマンドは、IPv6 ネイバー探索キャッシュ内のスタティック エントリを表示するために使用します。IPv6 ネイバー探索キャッシュ内のスタティック エントリは次のいずれかの状態になります。

- INCMP (不完全) : このエントリのインターフェイスがダウンしています。
- REACH (到達可能) : このエントリのインターフェイスがアップしています。



Note 到達可能性検出は、IPv6 ネイバー探索キャッシュ内のスタティック エントリに適用されません。そのため、INCMP および REACH 状態に関する説明とダイナミックおよびスタティック キャッシュ エントリに関する説明は一致しません。ダイナミック キャッシュ エントリの INCMP ステータスおよび REACH ステータスの説明については、**show ipv6 neighbors** コマンドを参照してください。

clear ipv6 neighbors コマンドは、スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべての エントリを削除します。**no ipv6 neighbor** コマンドは、指定されたスタティック エントリをネイバー探索キャッシュから削除します。IPv6 ネイバー探索プロセスで学習されたダイナミック エントリはキャッシュから削除されません。**no ipv6 enable** コマンドまたは **no ipv6 unnumbered** コマンドを使用してインターフェイスで IPv6 を無効にすると、スタティック エントリを除き、そのインターフェイス用に設定したすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP に変更されます）。

IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。



Note IPv6 隣接のスタティック エントリは、IPv6 がイネーブルにされている LAN および ATM LAN Emulation インターフェイスだけで設定できます。

Examples

次の例では、イーサネット インターフェイス 1 上の IPv6 アドレスが 2001:0DB8::45A で、リンク層アドレスが 0002.7D1A.9472 のネイバーに関する IPv6 ネイバー探索キャッシュ内の静的 エントリを設定します。

```
デバイス(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```

Related Commands

コマンド	説明
arp (global)	パーマネント エントリを ARP キャッシュに追加します。
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべての エントリを削除します。
no ipv6 enable	明示的な IPv6 アドレスで設定されていないインターフェイスでの IPv6 処理をディセーブルにします。
no ipv6 unnumbered	アンナンバード インターフェイス上の IPv6 を無効にします。
show ipv6 neighbors	IPv6 ネイバー探索キャッシュ情報を表示します。

ipv6 ospf name-lookup

Open Shortest Path First (OSPF) ルータ ID をドメインネームシステム (DNS) 名として表示するには、グローバル コンフィギュレーション モードで **ipv6 ospf name-lookup** コマンドを使用します。DNS 名として OSPF ルータ ID の表示を停止するには、このコマンドの **no** 形式を使用します。

ipv6 ospf name-lookup
no ipv6 ospf name-lookup

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default このコマンドはデフォルトでは無効になっています。

Command Modes グローバル コンフィギュレーション (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドを使用するとルータがルータ ID やネイバー ID ではなく名前が表示されるため、ルータを識別しやすくなります。

Examples

次に、すべての OSPF show EXEC コマンドの表示で使用する DNS 名を検索するように OSPF を設定する例を示します。

```
デバイス(config)# ipv6 ospf name-lookup
```

ipv6 pim

IPv6 Protocol Independent Multicast (PIM) を指定したインターフェイス上で再度有効にするには、インターフェイス コンフィギュレーション モードで **ipv6 pim** コマンドを使用します。指定したインターフェイス上で PIM を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 pim
no ipv6 pim

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default PIM はすべてのインターフェイス上で自動的に有効になります。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 multicast-routing** コマンドを有効にすると、PIM はすべてのインターフェイス上で実行できるようになります。PIM はデフォルトですべてのインターフェイス上で有効になるため、**ipv6 pim** コマンドの **no** 形式を使用し、指定したインターフェイス上で PIM を無効にします。PIM がインターフェイス上で無効になっている場合は、マルチキャストリスナー検出 (MLD) プロトコルからのホスト メンバーシップ通知に反応しません。

Examples

次に、ファストイーサネットインターフェイス 1/0 で PIM をオフにする例を示します。

```
デバイス(config)# interface FastEthernet 1/0
デバイス(config-if)# no ipv6 pim
```

Related Commands	コマンド	説明
	ipv6 multicast-routing	ルータのすべての IPv6 対応インターフェイス上で PIM と MLD を使用したマルチキャストルーティングを有効にし、マルチキャスト転送を有効にします。

ipv6 pim accept-register

ランデブーポイント（RP）で登録を承認または拒否するには、グローバルコンフィギュレーションモードで **ipv6 pim accept-register** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
ipv6 pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
no ipv6 pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
```

Syntax Description	Parameter	Description
	vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
	list <i>access-list</i>	アクセスリスト名を定義します。
	route-map <i>map-name</i>	ルートマップを定義します。

Command Default すべての送信元が RP で承認されます。

Command Modes グローバル コンフィギュレーション（config）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 名前付きのアクセスリストまたはルートマップを一致属性で設定するには、**ipv6 pim accept-register** コマンドを使用します。*access-list* 引数と *map-name* 引数で定義された permit 条件が満たされている場合、登録メッセージは承認されます。それ以外の場合、登録メッセージは承認されず、即時登録停止メッセージがカプセル化する宛先ルータに返されます。

Examples

次に、ローカルマルチキャストルートが備わっていないすべての送信元上でフィルタ処理する例を示します。

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
  match as-path 101
ip as-path access-list 101 permit
```

ipv6 pim allow-rp

PIM Allow RP 機能を IPv6 デバイス内のすべての IP マルチキャスト対応のインターフェイスに有効にするには、グローバル コンフィギュレーションモードで **ip pim allow-rp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 pim allow-rp [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
no ipv6 pim allow-rp

Syntax Description	
group-list	(任意) PIM Allow RP に許可されたグループ範囲のアクセス コントロール リスト (ACL) を指定します。
rp-list	(任意) PIM Allow RP に許可されたランデブー ポイント (RP) アドレスの ACL を指定します。
access-list	(任意) 標準 ACL の固有番号または固有名。

Command Default PIM Allow RP は無効になっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドを使用して、IP マルチキャストネットワーク内の受信側デバイスを有効にして、予期しない (別の) RP アドレスからの (*, G) join を承認します。

PIM Allow RP を有効にする前に、最初に **ipv6 pim rp-address** コマンドを使用して RP を定義する必要があります。

Related Commands	コマンド	説明
	ipv6 pim rp-address	マルチキャストグループの PIM RP のアドレスを静的に設定します。

ipv6 pim neighbor-filter list

特定の IPv6 アドレスからの Protocol Independent Multicast (PIM) ネイバーメッセージをフィルタ処理するには、グローバル コンフィギュレーション モードで **ipv6 pim neighbor-filter** コマンドを使用します。ルータをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
ipv6 pim [vrf vrf-name] neighbor-filter list access-list
no ipv6 pim [vrf vrf-name] neighbor-filter list access-list
```

Syntax Description		
vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。	
<i>access-list</i>	送信元からの PIM の hello パケットを拒否する IPv6 アクセス リストの名前。	

Command Default PIM ネイバー メッセージはフィルタリングされません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **ipv6 pim neighbor-filter list** コマンドは、LAN 上の不正ルータが PIM ネイバーになるのを防止するために使用します。このコマンドで指定されているアドレスからの hello メッセージが無視されます。

Examples

次に、PIM に IPv6 アドレス FE80::A8BB:CCFF:FE03:7200: からのすべての hello メッセージを無視させる例を示します。

```
デバイス(config)# ipv6 pim neighbor-filter list nbr_filter_acl
デバイス(config)# ipv6 access-list nbr_filter_acl
デバイス(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
デバイス(config-ipv6-acl)# permit any any
```

ipv6 pim rp-address

特定のグループ範囲に Protocol-Independent Multicast (PIM) ランデブーポイント (RP) のアドレスを設定するには、グローバルコンフィギュレーションモードで **ipv6 pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]
no ipv6 pim rp-address ipv6-address [group-access-list] [bidir]
```

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>ipv6-address</i>	PIM RP になるルータの IPv6 アドレス。 <i>ipv6-address</i> 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
<i>group-access-list</i>	(任意) RP をどのマルチキャスト グループに使用するかを定義するアクセスリストの名前。 アクセスリストに割り当てられた Source-Specific Multicast (SSM) グループアドレスの範囲 (FF3x::/96) に重複するグループアドレスの範囲が含まれている場合、警告メッセージが表示され、重複する範囲は無視されます。アクセスリストを指定しない場合は、有効なマルチキャスト非 SSM アドレスのすべての範囲に指定した RP が使用されます。 組み込み RP をサポートするには、RP として設定したルータが、組み込み RP アドレスから生成した組み込み RP グループの範囲を許可する設定済みのアクセスリストを使用する必要があります。 組み込み RP グループの範囲にすべての範囲 (3 ~ 7 など) を含める必要はありません。
bidir	(任意) 双方向共有ツリー転送に使用するグループ範囲を指定します。指定しないと、スパースモード転送に使用されます。単一の IPv6 アドレスは、双方向またはスパースモード範囲のいずれかにのみ RP として設定できます。単一のグループ範囲リストは、双方向モードかスパースモードのいずれかで動作するように設定できます。

Command Default

PIM RP は事前に設定されていません。組み込み RP サポートは、IPv6 PIM が有効になっている (組み込み RP サポートが提供される) 場合に、デフォルトで有効になります。マルチキャストグループは PIM スパースモードで動作します。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

PIM がスパース モードで設定されている場合は、RP として動作する 1 つ以上のルータを選択する必要があります。RP は、共有配布ツリーの唯一かつ共通のルートで、各ルータではスタティックに設定されます。

組み込み RP サポートが利用できる場合、RP を組み込み RP 範囲の RP として静的に設定する必要があります。他の IPv6 PIM ルータでのその他の設定は必要ありません。他のルータは、IPv6 グループアドレスから RP アドレスを検出します。これらのルータが組み込み RP の代わりに静的 RP を選択する場合、特定の組み込み RP グループ範囲を静的 RP のアクセス リストに設定する必要があります。

送信元マルチキャスト ホストの代わりに、ファーストホップ ルータが使用する RP アドレスを使用して登録パケットを送信します。また、グループのメンバにするマルチキャストホストの代わりに、ルータが RP アドレスを使用します。これらのルータは join メッセージと prune メッセージを RP に送信します。

オプションの *group-access-list* 引数を指定しないと、FFX[3-f]::/8 ~ FF3X::/96 の範囲の SSM を除き、ルーティング可能な IPv6 マルチキャスト グループの範囲全体に RP が適用されます。

group-access-list 引数を指定した場合、IPv6 アドレスは *group-access-list* 引数内に指定したグループの範囲の RP アドレスになります。

複数のグループに単一の RP を使用するように Cisco IOS ソフトウェアを設定できます。アクセス リストで指定されている条件によって、RP を使用できるグループが決定されます。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。

PIM ルータは複数の RP を使用できますが、グループごとに 1 つのみです。

Examples

次に、すべてのマルチキャスト グループの PIM RP アドレスを 2001::10:10 に設定する例を示します。

```
デバイス(config)# ipv6 pim rp-address 2001::10:10
```

次に、マルチキャスト グループ FF04::/64 についてのみ PIM RP アドレスを 2001::10:10 に設定する例を示します。

```
デバイス(config)# ipv6 access-list acc-grp-1
デバイス(config-ipv6-acl)# permit ipv6 any ff04::/64
デバイス(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

次に、IPv6 アドレス 2001:0DB8:2::2 から生成した組み込み RP の範囲を許可するグループ アクセス リストを設定する例を示します。

```
デバイス(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
デバイス(config)# ipv6 access-list embd-ranges
デバイス(config-ipv6-acl)# permit ipv6 any ff73:240:2:2::/96
```

```

デバイス(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
デバイス(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
デバイス(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
デバイス(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
デバイス(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96

```

次に、アドレス 100::1 をマルチキャスト範囲 FF::8 全体の双方向 RP として有効にする例を示します。

```
ipv6 pim rp-address 100::1 bidir
```

次に、IPv6 アドレス 200::1 を、bidir-grps というアクセスリストで許可された範囲の双方向 RP として有効にする例を示します。このリストで許可された範囲は ff05::/16 と ff06::/16 です。

```

デバイス(config)# ipv6 access-list bidir-grps
デバイス(config-ipv6-acl)# permit ipv6 any ff05::/16
デバイス(config-ipv6-acl)# permit ipv6 any ff06::/16
デバイス(config-ipv6-acl)# exit
デバイス(config)# ipv6 pim rp-address 200::1 bidir-grps bidir

```

Related Commands

コマンド	説明
debug ipv6 pim df-election	PIM 双方向 DF 選択メッセージ処理のデバッグメッセージを表示します。
ipv6 access-list	IPv6 アクセスリストを定義し、ルータを IPv6 アクセスリスト コンフィギュレーションモードにします。
show ipv6 pim df	各 RP の各インターフェイスの DF 選択状態を表示します。
show ipv6 pim df winner	各 RP の各インターフェイスの DF 選択ウィナーを表示します。

ipv6 pim rp embedded

IPv6 Protocol Independent Multicast (PIM) で組み込みランデブーポイント (RP) サポートを有効にするには、グローバル コンフィギュレーション モードで **ipv6 pim rp-embedded** コマンドを使用します。組み込み RP サポートを無効にするには、このコマンドの **no** 形式を使用します。

```
ipv6 pim [vrf vrf-name] rp embedded
no ipv6 pim [vrf vrf-name] rp embedded
```

Syntax Description	<table border="1"> <tr> <td>vrf <i>vrf-name</i></td> <td>(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。</td> </tr> </table>	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。		

Command Default 組み込み RP サポートはデフォルトで有効になっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines 組み込み RP サポートはデフォルトで有効になるため、組み込み RP サポートをオフにするには、ユーザは通常、このコマンドの **no** 形式を使用します。

ipv6 pim rp embedded コマンドは、組み込み RP グループ範囲の ff7X::/16 と fffX::/16 にのみ適用されます。ルータが有効になっている場合、組み込み RP グループ範囲の ff7X::/16 と fffX::/16 のグループを解析し、使用する RP をグループ アドレスから抽出します。

Examples

次に、IPv6 PIM の組み込み RP サポートを無効にする例を示します。

```
デバイス# no ipv6 pim rp embedded
```

ipv6 pim spt-threshold infinity

Protocol Independent Multicast (PIM) リーフルータが指定したグループの最短パスツリー (SPT) にいつ参加するかを設定するには、グローバル コンフィギュレーション モードで **ipv6 pim spt-threshold infinity** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 pim [vrf vrf-name] spt-threshold infinity [group-list access-list-name]
no ipv6 pim spt-threshold infinity

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
group-list <i>access-list-name</i>	(任意) しきい値を適用するグループを指定します。標準的な IPv6 アクセスリスト名である必要があります。この値を省略すると、すべてのグループにしきい値が適用されます。

Command Default

このコマンドを使用しない場合、最初のパケットが新しい送信元から到着するとすぐに、PIM リーフルータが SPT に参加します。ルータが SPT に参加した後では、**ipv6 pim spt-threshold infinity** コマンドによって共有ツリーに切り替わりません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 pim spt-threshold infinity コマンドを使用すると、共有ツリーを使用するよう指定したグループのすべての送信元が有効になります。**group-list** キーワードは、SPT しきい値を適用するグループを指定します。

access-list-name 引数は IPv6 アクセスリストを参照します。*access-list-name* 引数を値 0 で指定するか、または **group-list** キーワードを使用しない場合は、SPT しきい値がすべてのグループに適用されます。デフォルト設定 (このコマンドが無効になっている) では、新しい送信元から最初のパケットが着信した直後に SPT に参加します。

Examples

次に、PIM のラストホップルータが共有ツリーに留まり、グループの範囲の ff04::/64 の SPT に切り替わらない例を示します。

```

デバイス(config)# ipv6 access-list acc-grp-1
デバイス(config-ipv6-acl)# permit ipv6 any FF04::/64
デバイス(config-ipv6-acl)# exit
デバイス(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1

```

ipv6 prefix-list

IPv6プレフィックスリストのエントリを作成するには、グローバルコンフィギュレーションモードで **ipv6 prefix-list** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

```

ipv6 prefix-list list-name [seq seq-number] {deny ipv6-prefix/prefix-length | permit
ipv6-prefix/prefix-length | description text} [ge ge-value] [le le-value]
no ipv6 prefix-list list-name
  
```

Syntax Description

<i>list-name</i>	プレフィックス リストの名前。 <ul style="list-style-type: none"> 既存のアクセス リストと同じ名前にはできません。 show ipv6 prefix-list コマンドのキーワードであるため、名前に「detail」や「summary」を使用することはできません。
seq <i>seq-number</i>	(オプション) 設定するプレフィックス リスト エントリのシーケンス番号。
deny	条件に一致するネットワークを拒否します。
permit	条件に一致するネットワークを許可します。
<i>ipv6-prefix</i>	指定したプレフィックス リストに割り当てられている IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>/prefix-length</i>	IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
description <i>text</i>	プレフィックス リストの説明。最大 80 文字です。
ge <i>ge-value</i>	(任意) <i>ipv6-prefix/prefix-length</i> 引数の値と等しいかそれよりも長いプレフィックス長を指定します。これは <i>length</i> の範囲の最小値です (長さ範囲の「下限」に該当する値)。
le <i>le-value</i>	(任意) <i>ipv6-prefix/prefix-length</i> 引数の値と等しいかそれよりも短いプレフィックス長を指定します。これは <i>length</i> の範囲の最大値です (長さ範囲の「上限」に該当する値)。

Command Default

プレフィックス リストは作成されません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 prefix-list コマンドは、IPv6 固有である点を除いて、**ip prefix-list** コマンドに似ています。

ネットワークが更新でアドバタイズされることを抑制するには、**distribute-list out** コマンドを使用します。

プレフィックスリストエントリのシーケンス番号によって、リスト中のエントリの順番が決まります。ルータは、ネットワーク アドレスとプレフィックス リスト エントリを比較します。ルータは、プレフィックス リストの先頭（最も小さいシーケンス番号）から比較を開始します。

プレフィックス リストの複数のエントリがプレフィックスに一致する場合、シーケンス番号が最も小さいエントリが実際の一致と見なされます。一致または拒否が発生すると、プレフィックス リストの残りのエントリは処理されません。効率を向上させるため、*seq-number* 引数を使用して最も一般的な **permit** や **deny** をリストの最上部近くに配置できます。

show ipv6 prefix-list コマンドを使用すると、エントリのシーケンス番号が表示されます。

IPv6 プレフィックス リストは、**permit** 文または **deny** 文を適用する前に照合が必要な特定のプレフィックスまたはプレフィックスの範囲を指定するために使用されます。2つのオペランド キーワードを使用して、照合するプレフィックス長の範囲を指定できます。ある値以下のプレフィックス長は、**le** キーワードで設定します。ある値以上のプレフィックス長は、**ge** キーワードを使用して指定します。**ge** および **le** キーワードを使用すると、通常の *ipv6-prefix/prefix-length* 引数よりも詳細に、照合するプレフィックス長の範囲を指定できます。プレフィックス リストのエントリと照合される候補プレフィックスに対して、次の3つの条件が存在する可能性があります。

- 候補プレフィックスは、指定したプレフィックス リストおよびプレフィックス長エントリと一致している必要があります。
- 省略可能な **le** キーワードの値によって、許可されるプレフィックス長が、*prefix-length* 引数から **le** キーワードの値（この値を含む）までの範囲で指定されます。
- 省略可能な **ge** キーワードの値によって、許可されるプレフィックス長が、**ge** キーワードの値から 128（この値を含む）までの範囲で指定されます。



Note 最初の条件は、他の条件が有効になる前に一致している必要があります。

ge または **le** キーワードを指定しなかった場合は、完全一致であると想定されます。1つのキーワード オペランドだけを指定した場合、そのキーワードの条件が適用され、もう1つの条件は適用されません。*prefix-length* 値は、**ge** 値よりも小さい必要があります。**ge** 値は、**le** 値以下である必要があります。**le** 値は、128 以下である必要があります。

すべての IPv6 プレフィックス リスト（許可および拒否の条件文が含まれていないプレフィックス リストを含む）には、最後の一致条件として暗黙の **deny any any** ステートメントが含まれていません。

Examples

次に、プレフィックス `::/0` を持つすべてのルートを拒否する例を示します。

```
デバイス(config)# ipv6 prefix-list abc deny ::/0
```

次に、プレフィックス `2002::/16` を許可する例を示します。

```
デバイス(config)# ipv6 prefix-list abc permit 2002::/16
```

次に、プレフィックス `5F00::/48` 以上でプレフィックス `5F00::/64` を含むすべてのプレフィックスを承認するプレフィックスのグループを指定する例を示します。

```
デバイス(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

次に、プレフィックス `2001:0DB8::/64` を持つルート内の 64 ビットよりも大きいプレフィックス長を拒否する例を示します。

```
デバイス(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

次に、すべてのアドレス空間で 32 ~ 64 ビットのマスク長を許可する例を示します。

```
デバイス(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

次に、すべてのアドレス空間で 32 ビットよりも大きいマスク長を拒否する例を示します。

```
デバイス(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

次に、プレフィックス `2002::/128` を持つすべてのルートを拒否する例を示します。

```
デバイス(config)# ipv6 prefix-list abc deny 2002::/128
```

次に、プレフィックス `::/0` を持つすべてのルートを許可する例を示します。

```
デバイス(config)# ipv6 prefix-list abc permit ::/0
```

Related Commands

コマンド	説明
clear ipv6 prefix-list	IPv6 プレフィックス リスト エントリの ヒット カウント をリセット します。
distribute-list out	ネットワーク が更新 時に アドバタイズ されない ように します。
ipv6 prefix-list sequence-number	IPv6 プレフィックス リスト 内の エントリ の シーケンス 番号 の 生成 を有効 に します。
match ipv6 address	プレフィックス リスト によって 許可 される プレフィックス を持つ IPv6 ルート を 配信 します。
show ipv6 prefix-list	IPv6 プレフィックス リスト または IPv6 プレフィックス リスト の エントリ に関する 情報 を 表示 します。

ipv6 source-guard attach-policy

インターフェイス上の IPv6 送信元ガードポリシーを適用するには、インターフェイス コンフィギュレーションモードで **ipv6 source-guard attach-policy** を使用します。インターフェイスから送信元ガードを削除するには、このコマンドの **no** 形式を使用します。

ipv6 source-guard attach-policy[*source-guard-policy*]

Syntax Description

<i>source-guard-policy</i>	(任意) 送信元ガード ポリシーのユーザ定義名。ポリシー名には象徴的な文字列 (Engineering など) または整数 (0 など) を使用できます。
----------------------------	---

Command Default

IPv6 送信元ガード ポリシーはインターフェイスに適用されません。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

source-guard-policy 引数を使用してポリシーを指定しないと、デフォルトの送信元ガードポリシーが適用されます。

IPv6 送信元ガードと IPv6 スヌーピング間には依存関係があります。IPv6 送信元ガードが設定されるたびに、**ipv6 source-guard attach-policy** コマンドが入力されると、スヌーピングが有効になっていることを確認し、有効になっていない場合は警告を発行します。IPv6 スヌーピングが無効になっている場合、ソフトウェアは IPv6 送信元ガードが有効になっていることを確認し、有効になっていれば警告を送信します。

Examples

次に、インターフェイスに IPv6 送信元ガードを適用する例を示します。

```
デバイス(config)# interface gigabitethernet 0/0/1
デバイス(config-if)# ipv6 source-guard attach-policy mysnoopingpolicy
```

Related Commands

コマンド	説明
ipv6 snooping policy	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始します。

ipv6 source-route

IPv6 タイプ 0 のルーティングヘッダー（IPv6 送信元ルーティングヘッダー）の処理を有効にするには、グローバル コンフィギュレーション モードで **ipv6 source-route** コマンドを使用します。IPv6 拡張ヘッダーの処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 source-route
no ipv6 source-route

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

デフォルトは、**ipv6 source-route** コマンドの **no** バージョンです。ルータがタイプ 0 のルーティングヘッダーを持つパケットを受信すると、そのルータはパケットをドロップして IPv6 Internet Control Message Protocol (ICMP) エラーメッセージを送信元に送り返し、適切なデバッグメッセージをログに記録します。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デフォルトが **ipv6 source-route** コマンドの **no** バージョンに変更されました。つまり、この機能は有効になっていません。この変更以前は、この機能は自動的に有効になっていました。デフォルトが変更される前に **no ipv6 source-route** コマンドを設定した場合、このコマンドの **no** バージョンがデフォルトであるとしても、**show config** コマンドの出力内にこの設定が引き続き表示されます。

no ipv6 source-route コマンド（デフォルト）は、ホストがルータを使用して送信元ルーティングを実行しないようにします。**no ipv6 source-route** コマンドが設定されている場合に、ルータが type0 の送信元ルーティングヘッダーを持つパケットを受信すると、ルータはそのパケットをドロップして、送信元に IPv6 ICMP エラーメッセージを返信し、適切なデバッグメッセージを記録します。

IPv6 では、パケットの宛先によってのみ、送信元ルーティングが実行されます。そのため、送信元ルーティングがネットワーク内で実行されないようにするには、次のルールを含む IPv6 アクセスコントロールリスト (ACL) を設定する必要があります。

```
deny ipv6 any any routing
```

ルータが IPv6 ICMP エラーメッセージを生成するレートを制限するには、**ipv6 icmp error-interval** コマンドを使用します。

Examples

次に、IPv6 タイプ 0 のルーティングヘッダーの処理を無効にする例を示します。

```
no ipv6 source-route
```

Related Commands

コマンド	説明
deny (IPv6)	IPv6 アクセス リストに拒否条件を設定します。
ipv6 icmp error-interval	IPv6 ICMP エラーメッセージの間隔を設定します。

ipv6 spd mode

IPv6 選択的パケット破棄 (SPD) モードを設定するには、グローバル コンフィギュレーション モードで **ipv6 spd mode** コマンドを使用します。IPv6 SPD モードを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 spd mode {aggressive|tos protocol ospf}
no ipv6 spd mode {aggressive|tos protocol ospf}
```

Syntax Description	aggressive	aggressive drop モードでは、IPv6 SPD が random drop 状態の場合にフォーマットに誤りのあるパケットがドロップされます。
	tos protocol ospf	OSPF モードでは、SPD 優先度で処理する OSPF パケットを使用できます。

Command Default IPv6 SPD モードは設定されません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines IPv6 SPD モードのデフォルト設定はありませんが、**ipv6 spd mode** コマンドを使用して、特定の SPD 状態に到達したときに使用するモードを設定できます。

aggressive キーワードは、IPv6 SPD が random drop 状態のときにフォーマットが崩れているパケットをドロップする aggressive drop モードを有効にします。**ospf** キーワードは、OSPF パケットを SPD 優先度で処理する OSPF モードを有効にします。

プロセス入力キューのサイズによって SPD ステートが normal (ドロップなし) か、random drop か、max かが決まります。プロセス入力キューが SPD の最小しきい値よりも小さい場合、SPD は何も行わず、normal ステートになります。normal ステートでは、パケットはドロップされません。入力キューが最大しきい値に到達すると、SPD は max ステートになります。このステートでは、通常プライオリティのパケットが破棄されます。入力キューが最小しきい値と最大しきい値の間にある場合、SPD は random drop ステートになります。このステートでは、通常パケットがドロップされることがあります。

Examples

次に、ルータが random drop 状態のときにフォーマットが崩れたパケットをルータでドロップできるようにする例を示します。

```
デバイス (config) # ipv6 spd mode aggressive
```

Related Commands

コマンド	説明
ipv6 spd queue max-threshold	IPv6 SPD プロセス入力キュー内の最大パケット数を設定します。
ipv6 spd queue min-threshold	IPv6 SPD プロセス入力キュー内の最小パケット数を設定します。
show ipv6 spd	IPv6 SPD 設定を表示します。

ipv6 spd queue max-threshold

IPv6 選択的パケット破棄（SPD）プロセスの入力キュー内のパケットの最大数を設定するには、グローバル コンフィギュレーション モードで **ipv6 spd queue max-threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 spd queue max-threshold *value*
no ipv6 spd queue max-threshold

Syntax Description	<i>value</i>	パケット数。指定できる範囲は 0 ~ 65535 です。
---------------------------	--------------	------------------------------

Command Default SPD キューの最大しきい値は設定されません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines SPD キューの最大しきい値を設定するには、**ipv6 spd queue max-threshold** コマンドを使用します。プロセス入力キューのサイズによって SPD ステートが **normal**（ドロップなし）か、**random drop** か、**max** かが決まります。プロセス入力キューが SPD の最小しきい値よりも小さい場合、SPD は何も行わず、**normal** ステートになります。**normal** ステートでは、パケットはドロップされません。入力キューが最大しきい値に到達すると、SPD は **max** ステートになります。このステートでは、通常プライオリティのパケットが破棄されます。入力キューが最小しきい値と最大しきい値の間にある場合、SPD は **random drop** ステートになります。このステートでは、通常パケットがドロップされることがあります。

Examples

次に、キューの最大しきい値を 60,000 に設定する例を示します。

```
デバイス(config)# ipv6 spd queue max-threshold 60000
```

Related Commands	コマンド	説明
	ipv6 spd queue min-threshold	IPv6 SPD プロセス入力キュー内の最小パケット数を設定します。
	show ipv6 spd	IPv6 SPD 設定を表示します。

ipv6 traffic interface-statistics

すべてのインターフェイスのIPv6転送統計を収集するには、グローバルコンフィギュレーションモードで **ipv6 traffic interface-statistics** コマンドを使用します。どのインターフェイスのIPv6転送統計も収集しないようにするには、このコマンドの **no** 形式を使用します。

ipv6 traffic interface-statistics [unclearable]
no ipv6 traffic interface-statistics [unclearable]

Syntax Description

unclearable	(任意) IPv6 転送統計はすべてのインターフェイスについて保管されますが、任意のインターフェイスの統計をクリアすることはできません。
--------------------	--

Command Default

IPv6 転送統計は、すべてのインターフェイスについて収集されます。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

オプションの **unclearable** キーワードを使用すると、インターフェイスごとの統計ストレージの要件が半減します。

Examples

次に、任意のインターフェイス上で統計をクリアできないようにする例を示します。

```
デバイス(config)# ipv6 traffic interface-statistics unclearable
```

ipv6 unicast-routing

IPv6 ユニキャストデータグラムの転送を有効にするには、グローバル コンフィギュレーション モードで **ipv6 unicast-routing** コマンドを使用します。IPv6 ユニキャストデータグラムの転送を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 unicast-routing
no ipv6 unicast-routing

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IPv6 ユニキャスト ルーティングはディセーブルに設定されています。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

no ipv6 unicast-routing コマンドを設定すると、IPv6 ルーティングテーブルから IPv6 ルーティングプロトコルのすべてのエントリが削除されます。

Examples

次に、IPv6 ユニキャスト データグラムの転送を有効にする例を示します。

```
デバイス(config)# ipv6 unicast-routing
```

Related Commands

コマンド	説明
ipv6 address link-local	インターフェイスの IPv6 リンクローカルアドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 enable	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 route	IPv6 ルーティングテーブルの現在の内容を表示します。

key chain

ルーティングプロトコルの認証を有効にするために必要な認証キーチェーンを定義して、キーチェーン コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **key chain** コマンドを使用します。キーチェーンを削除するには、このコマンドの **no** 形式を使用します。

key chain *name-of-chain*
no key chain *name-of-chain*

Syntax Description

<i>name-of-chain</i>	キーチェーンの名前。キーチェーンには、少なくとも1つのキーを含める必要がありますが、最大 2147483647 個のキーを含めることができます。
----------------------	--

Command Default

キーチェーンは存在しません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

認証を有効にするには、キーでキーチェーンを設定する必要があります。

複数のキーチェーンの識別が可能です。ルーティングプロトコルごとのインターフェイスごとに1つのキーチェーンを使用することを推奨します。**key chain** コマンドを指定すると、キーチェーン コンフィギュレーション モードが開始されます。

Examples

次に、キーチェーンを指定する例を示します。

```
Device(config-keychain-key)# key-string chestnut
```

Related Commands

Command	Description
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
key	キーチェーンの認証キーを識別します。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

key-string (認証)

キーの認証文字列を指定するには、キーチェーンキーコンフィギュレーションモードで **key-string** (認証) コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

key-string **key-string** *text*
no **key-string** *text*

Syntax Description

<i>text</i>	認証されるルーティングプロトコルを使用してパケットで送信および受信される必要のある認証文字列。文字列には、大文字小文字の英数字 1～80 文字を含めることができます。
-------------	---

Command Default

キーの認証文字列は存在しません。

Command Modes

キーチェーンキーコンフィギュレーション (config-keychain-key)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、キーの認証文字列を指定する例を示します。

```
Device(config-keychain-key)# key-string key1
```

Related Commands

Command	Description
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
key	キーチェーンの認証キーを識別します。
key chain	ルーティングプロトコルの認証をイネーブルにするために必要な認証キーチェーンを定義します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

key

キーチェーンの認証キーを識別するには、キーチェーン コンフィギュレーション モードで **key** コマンドを使用します。キーチェーンからキーを削除するには、このコマンドの **no** 形式を使用します。

key *key-id*

no key *key-id*

Syntax Description

<i>key-id</i>	キーチェーンの認証キーの識別番号。キーの範囲は 0 ～ 2147483647 です。キーの ID 番号は連続している必要はありません。
---------------	---

Command Default

キーチェーンにキーは存在しません。

Command Modes

キーチェーン コンフィギュレーション (config-keychain)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

キーチェーンに複数のキーを設定し、**accept-lifetime** および **send-lifetime** キーチェーンキー コマンド設定に基づいてキーが将来無効になるように、ソフトウェアでキーを配列できるようにすると便利です。

各キーには、ローカルに格納される独自のキー識別子があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5 (MD5) 認証キーが一意に識別されます。有効なキーの数にかかわらず、1 つの認証パケットのみが送信されます。ソフトウェアは、最小のキー識別番号の検索を開始し、最初の有効なキーを使用します。

最後のキーが期限切れになった場合、認証は続行されますが、エラーメッセージが生成されません。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

すべてのキーを削除するには、**no key chain** コマンドを使用してキーチェーンを削除します。

Examples

次に、キーを指定してキーチェーンでの認証を確認する例を示します。

```
Device (config-keychain) # key 1
```

Related Commands

Command	Description
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。

Command	Description
key chain	ルーティングプロトコルの認証をイネーブルにするために必要な認証キー チェーンを定義します。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キー チェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

show ip ports all

デバイス上で開いているすべてのポートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip ports all** を使用します。

show ip ports all

Syntax Description

構文の説明

このコマンドには引数またはキーワードはありません。

Command Default

デフォルトの動作や値はありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、Cisco ネットワーキング スタックを使用して開かれたポートを含むシステム上で開いているすべての TCP/IP ポートのリストを表示します。

開いているポートを閉じるには、次のいずれかの方法を使用します。

- アクセスコントロールリスト (ACL) を使用します。
- UDP 2228 ポートを閉じるには、**no l2 traceroute** コマンドを使用します。
- TCP 80、TCP 443、TCP 6970、TCP 8090 ポートを閉じるには、**no ip http server** および **no ip http secure-server** コマンドを使用します。

Examples

次に、**show ip ports all** コマンドの出力例を示します。

```
Device#
show ip ports all
Proto Local Address Foreign Address State PID/Program Name
TCB Local Address Foreign Address (state)
tcp *:4786 *:* LISTEN 224/[IOS]SMI IBC server process
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
udp *:10002 *:* 0/[IOS] Unknown
udp *:2228 10.0.0.0:0 318/[IOS]L2TRACE SERVER
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 29: show ip ports all のフィールドの説明

フィールド	説明
Protocol	使用されている転送プロトコル。
Local Address.	デバイスの IP アドレス。
Foreign Address	リモートまたはピア アドレス。
State	接続の状態。リッスン、確立済み、または接続済みを選択できます。
PID/Program Name	プロセス ID または名前。

Related Commands

Command	Description
show tcp brief all	TCP 接続のエンドポイントに関する情報を表示します。
show ip sockets	IP ソケット情報を表示します。

show ipv6 access-list

現在のすべての IPv6 アクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。

show ipv6 access-list [*access-list-name*]

Syntax Description

<i>access-list-name</i>	(任意) アクセスリストの名前
-------------------------	-----------------

Command Default

すべての IPv6 アクセス リストが表示されます。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 access-list コマンドは、IPv6 専用である点を除き、**show ip access-list** コマンドと同様の出力を提供します。

Examples

次の **show ipv6 access-list** コマンドの出力には、inbound、tcptraffic、および outbound という IPv6 アクセス リストが表示されます。

```

デバイス# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
  permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
  permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
  (time left 296) sequence 2
IPv6 access list outbound
  evaluate udptraffic
  evaluate tcptraffic

```

次に、IPSec で使用する IPv6 アクセス リスト情報を表示する例を示します。

```

デバイス# show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
  permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
  permit 89 FE80::/10 any (85 matches) sequence 1

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 30: show ipv6 access-list フィールドの説明

フィールド	説明
ipv6 access list inbound	IPv6 アクセス リスト名 (例: inbound)。
permit	指定されたプロトコル タイプと一致するパケットを許可します。
tcp	伝送制御プロトコル。パケットが一致しなければならない高いレベル (レイヤ 4) のプロトコル タイプ。
any	::/0 と同じです。
eq	TCP または UDP パケットの送信元または宛先ポートを比較する equal オペランド。
reflect	再帰 IPv6 アクセス リストを示します。
tcptraffic (8 matches)	再帰 IPv6 アクセス リストの名前と、そのアクセス リストの一致数。clear ipv6 access-list 特権 EXEC コマンドは IPv6 アクセス リストの一致カウンタをリセットします。
sequence 10	着信パケットが比較されるアクセス リストの行のシーケンス。アクセス リストの行は、最初のプライオリティ (最低の数、たとえば 10) から最後のプライオリティ (最高の数、たとえば 80) の順に並んでいます。
host 2001:0DB8:1::1	パケットの送信元アドレスが一致していなければならない送信元 IPv6 ホスト アドレス。
host 2001:0DB8:1::2	パケットの宛先アドレスが一致していなければならない宛先 IPv6 ホスト アドレス。
11000	発信接続用の一時送信元ポート番号。
timeout 300	tcptraffic という一時 IPv6 再帰アクセス リストが指定したセッションでタイムアウトするまでのアイドル時間の総間隔 (秒単位)。
(time left 243)	tcptraffic という一時 IPv6 再帰アクセス リストが指定したセッションで削除されるまでの残りのアイドル時間 (秒単位)。指定したセッションに一致する追加の受信トラフィックがこの値を 300 秒にリセットします。
evaluate udptraffic	udptraffic という IPv6 再帰アクセス リストが outbound という IPv6 アクセス リスト内に入れ子になっていることを示します。

Related Commands

コマンド	説明
clear ipv6 access-list	IPv6 アクセス リストの一致カウンタをリセットします。
hardware statistics	ハードウェア統計情報の収集をイネーブルにします。

コマンド	説明
show ip access-list	現在のすべての IP アクセス リストの内容を表示します。
show ip prefix-list	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストまたは IPv6 プレフィックス リストのエントリに関する情報を表示します。

show ipv6 destination-guard policy

宛先ガード情報を表示するには、特権 EXEC モードで **show ipv6 destination-guard policy** コマンドを使用します。

show ipv6 destination-guard policy [*policy-name*]

Syntax Description	<i>policy-name</i>	(任意) 宛先ガードポリシーの名前。
---------------------------	--------------------	--------------------

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines *policy-name* 引数を指定すると、指定したポリシー情報のみが表示されます。*policy-name* 引数を指定しないと、すべてのポリシーの情報が表示されます。

Examples

次に、ポリシーを VLAN に適用した場合の **show ipv6 destination-guard policy** コマンドの出力例を示します。

```
デバイス# show ipv6 destination-guard policy poll
Destination guard policy destination:
  enforcement always
  Target: vlan 300
```

次に、ポリシーをインターフェイスに適用した場合の **show ipv6 destination-guard policy** コマンドの出力例を示します。

```
デバイス# show ipv6 destination-guard policy poll
Destination guard policy destination:
  enforcement always
  Target: Gi0/0/1
```

Related Commands	コマンド	説明
	ipv6 destination-guard policy	宛先ガードポリシーを定義します。

show ipv6 dhcp

指定したデバイス上の Dynamic Host Configuration Protocol (DHCP) 固有識別子 (DUID) を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 dhcp** コマンドを使用します。

show ipv6 dhcp

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 dhcp コマンドは、クライアントとサーバの両方の ID に対して、リンク層アドレスに基づいた DUID を使用します。デバイスは、最も小さい番号のインターフェイスの MAC アドレスを使用して DUID を形成します。ネットワーク インターフェイスは、デバイスに永続的に接続されていると見なされます。デバイスの DUID を表示するには、**show ipv6 dhcp** コマンドを使用します。

Examples

次に、**show ipv6 dhcp** コマンドの出力例を示します。出力の内容は一目瞭然です。

```
デバイス# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

IPv6 サーバのバインディングテーブルの Dynamic Host Configuration Protocol (DHCP) から自動クライアントバインディングを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 dhcp binding** コマンドを使用します。

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description	
<i>ipv6-address</i>	(任意) IPv6 クライアントの DHCP のアドレス。
vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ipv6 dhcp binding** コマンドは、*ipv6-address* 引数を指定しないと、IPv6 サーババインディングテーブルの DHCP からすべての自動クライアントバインディングを表示します。*ipv6-address* 引数が指定されている場合、指定したクライアントのバインディングだけが表示されます。

vrf vrf-name キーワードと引数の組み合わせを使用すると、指定した VRF に属するすべてのバインディングが表示されます。



Note 設定した VRF が機能するには、**ipv6 dhcp server vrf enable** コマンドをイネーブルにしておく必要があります。このコマンドが設定されていない場合、**show ipv6 dhcp binding** コマンドの出力に設定した VRF が表示されず、デフォルトの VRF の詳細のみが表示されます。

Examples

次に、IPv6 サーババインディングテーブルの DHCP からすべての自動クライアントバインディングが表示された出力例を示します。

```

デバイス# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:300
DUID: 00030001AABBCC000300
Username : client_1
Interface: Virtual-Access2.1
IA PD: IA ID 0x000C0001, T1 75, T2 135
Prefix: 2001:380:E00::/64
        preferred lifetime 150, valid lifetime 300

```

show ipv6 dhcp binding

```

                expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
DUID: 00030001AABBCC000300
IA PD: IA ID 0x000D0001, T1 75, T2 135
Prefix: 2001:0DB8:E00:1::/64
                preferred lifetime 150, valid lifetime 300
                expires at Dec 06 2007 12:58 PM (288 seconds)

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 31: show ipv6 dhcp binding フィールドの説明

フィールド	説明
Client	指定したクライアントのアドレス。
DUID	DHCP 固有識別子 (DUID)。
Virtual-Access2.1	最初の仮想クライアント。IPv6 DHCP クライアントが2つのプレフィックスを要求し、そのプレフィックスの DUID が同じで、プレフィックス委任 (IAPD) に2つの異なるインターフェイスで異なる ID の関連付けがある場合、これらのプレフィックスは2つの異なるクライアント用として見なされ、両方のインターフェイス情報が保持されます。
Username : client_1	バインディングに関連付けられているユーザ名。
IA PD	クライアントに関連付けられているプレフィックスのコレクション。
IA ID	この IAPD の識別子。
Prefix	指定したクライアント上に指定された IAPD に委任されたプレフィックス。
preferred lifetime, valid lifetime	指定したクライアントの優先ライフタイムと有効なライフタイム設定 (秒単位)。
Expires at	有効なライフタイムの有効期限が切れる日時。
Virtual-Access2.2	2 番目の仮想クライアント。IPv6 DHCP クライアントが2つのプレフィックスを要求し、そのプレフィックスの DUID が同じで IAID が2つの異なるインターフェイス上で異なる場合、これらのプレフィックスは2つの異なるクライアント用と見なされ、両方のインターフェイス情報が保持されます。

Cisco IOS DHCPv6 サーバの DHCPv6 プールを設定して、認証、認可、およびアカウントिंग (AAA) サーバから委任のプレフィックスを取得すると、着信 PPP セッションから AAA サーバに PPP ユーザ名が送信され、プレフィックスを取得します。バインディングに関連付けられている PPP ユーザ名が **show ipv6 dhcp binding** コマンドの出力に表示されます。バインディングに関連付けられている PPP ユーザ名がない場合、このフィールドには値として「unassigned」が表示されます。

次に、バインディングに関連付けられている PPP ユーザ名が「client_1」である例を示します。

デバイス# **show ipv6 dhcp binding**

```
Client: FE80::2AA:FF:FE8B:CC
DUID: 0003000100AA00BB00CC
Username : client_1
Interface : Virtual-Access2
IA PD: IA ID 0x00130001, T1 75, T2 135
Prefix: 2001:0DB8:1:3::/80
        preferred lifetime 150, valid lifetime 300
        expires at Aug 07 2008 05:19 AM (225 seconds)
```

次に、バインディングに関連付けられている値が「unassigned」である例を示します。

デバイス# **show ipv6 dhcp binding**

```
Client: FE80::2AA:FF:FE8B:CC
DUID: 0003000100AA00BB00CC
Username : unassigned
Interface : Virtual-Access2
IA PD: IA ID 0x00130001, T1 150, T2 240
Prefix: 2001:0DB8:1:1::/80
        preferred lifetime 300, valid lifetime 300
        expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

Command	Description
ipv6 dhcp server vrf enable	DHCPv6 サーバ VRF 対応機能をイネーブルにします。
clear ipv6 dhcp binding	DHCP for IPv6 バインディング テーブルから自動クライアントバインディングを削除します。

show ipv6 dhcp conflict

アドレスがクライアントに提供されるときに Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが検出したアドレス競合を表示するには、特権 EXEC モードで **show ipv6 dhcp conflict** コマンドを使用します。

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description	
<i>ipv6-address</i>	（任意）IPv6 クライアントの DHCP のアドレス。
vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

Command Modes 特権 EXEC（#）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 競合を検出するように DHCPv6 サーバを設定する場合、DHCPv6 サーバは ping を使用します。クライアントはネイバー探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

Examples

次に、**show ipv6 dhcp conflict** コマンドの出力例を示します。このコマンドは DHCP 競合のプール値とプレフィックス値を表示します。

```
デバイス# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
      2001:0DB8:1005::10
```

Related Commands	コマンド	説明
	clear ipv6 dhcp conflict	DHCPv6 サーバデータベースからアドレス競合をクリアします。

show ipv6 dhcp database

Dynamic Host Configuration Protocol (DHCP) for IPv6 バインディング データベース エージェント情報を表示するには、ユーザ EXEC モードまたは特権モードで **show ipv6 dhcp database** コマンドを使用します。

show ipv6 dhcp database [*agent-URL*]

Syntax Description	
<i>agent-URL</i>	(任意) フラッシュ、NVRAM、FTP、TFTP、または Remote Copy Protocol (RCP) の Uniform Resource Locator。

Command Modes	ユーザ EXEC (>) 特権 EXEC (#)
---------------	-----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines バインディングデータベースが保存される永続的な各ストレージのことをデータベースエージェントと呼びます。エージェントを設定するには、**ipv6 dhcp database** コマンドを使用します。サポート対象のデータベースエージェントには、FTP サーバや TFTP サーバ、RCP、フラッシュファイルシステム、NVRAM などがあります。

show ipv6 dhcp database コマンドは、DHCP for IPv6 バインディング データベース エージェントの情報を表示します。*agent-URL* 引数が指定される場合、指定されたエージェントだけが表示されます。*agent-URL* 引数が指定されていない場合、すべてのデータベース エージェントが表示されます。

Examples

次に、**show ipv6 dhcp database** コマンドの出力例を示します。

```

デバイス# show ipv6 dhcp database
Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
  write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvrाम:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
  write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0

```

show ipv6 dhcp database

```

successful write times 3325
failed write times 0
Database agent flash:/dhcpv6-db:
write delay: 82 seconds, transfer timeout: 3 seconds
last written at Jan 09 2003 01:54 PM,
  write timer expires in 50 seconds
last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 32: show ipv6 dhcp database フィールドの説明

フィールド	説明
Database agent	データベース エージェントを指定します。
Write delay	データベースを更新するまでの待機時間（秒単位）。
transfer timeout	データベースの転送をキャンセルするまでに DHCP サーバが待機する時間（秒単位）を指定します。タイムアウト期間を超えた転送はキャンセルされます。
Last written	バインディングがファイルサーバに書き込まれた最後の日付と時刻。
Write timer expires...	書き込みタイマーの期限が切れるまでの時間（秒単位）。
Last read	バインディングがファイルサーバから読み取られた最後の日付と時刻。
Successful/failed read times	読み取りの成功回数と失敗回数。
Successful/failed write times	書き込みの成功回数と失敗回数。

Related Commands

Command	Description
ipv6 dhcp database	DHCP for IPv6 バインディング データベース エージェントのパラメータを指定します。

show ipv6 dhcp guard policy

Dynamic Host Configuration Protocol for IPv6（DHCPv6）ガード情報を表示するには、特権 EXEC モードで **show ipv6 dhcp guard policy** コマンドを使用します。

show ipv6 dhcp guard policy [*policy-name*]

Syntax Description

<i>policy-name</i>	(任意) DHCPv6 ガードポリシー名。
--------------------	-----------------------

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

policy-name 引数を指定すると、指定したポリシー情報のみが表示されます。*policy-name* 引数を指定しないと、すべてのポリシーの情報が表示されます。

Examples

次に、**show ipv6 dhcp guard guard** コマンドの出力例を示します。

```

デバイス# show ipv6 dhcp guard policy

Dhcp guard policy: default
  Device Role: dhcp client
  Target: Et0/3

Dhcp guard policy: test1
  Device Role: dhcp server
  Target: vlan 0   vlan 1   vlan 2   vlan 3   vlan 4
  Max Preference: 200
  Min Preference: 0
  Source Address Match Access List: acl1
  Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
  Device Role: dhcp relay
  Target: Et0/0 Et0/1 Et0/2

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 33: show ipv6 dhcp guard フィールドの説明

フィールド	説明
Device Role	デバイスのロール。ロールは、クライアント、サーバ、またはリレーのいずれかです。

show ipv6 dhcp guard policy

フィールド	説明
Target	ターゲットの名前。ターゲットは、インターフェイスまたは VLAN のいずれかです。

Related Commands

コマンド	説明
ipv6 dhcp guard policy	DHCPv6 ガード ポリシー名を定義します。

show ipv6 dhcp interface

Dynamic Host Configuration Protocol (DHCP) for IPv6 インターフェイス情報を表示するには、ユーザ EXEC モードまたは特権モードで **show ipv6 dhcp interface** コマンドを使用します。

show ipv6 dhcp interface [*type number*]

Syntax Description

<i>type number</i>	(任意) インターフェイスタイプおよび番号詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
--------------------	--

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

インターフェイスが指定されていない場合は、IPv6 用 DHCP (クライアントまたはサーバ) がイネーブルになっているすべてのインターフェイスが表示されます。インターフェイスが指定される場合、指定されているインターフェイスに関する情報だけが表示されます。

Examples

次に、**show ipv6 dhcp interface** コマンドの出力例を示します。最初の例では、DHCP for IPv6 サーバとして機能するインターフェイスを持つルータでコマンドを使用しています。2 番目の例では、DHCP for IPv6 クライアントとして機能するインターフェイスを持つルータでコマンドを使用しています。

```

デバイス# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-pl
  Preference value: 20
  Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEEA1:7439, DUID 000300010002FCA17400
    Preference: 20
    IA PD: IA ID 0x00040001, T1 120, T2 192
      Prefix: 3FFE:C00:C18:1::/72
        preferred lifetime 240, valid lifetime 54321
        expires at Nov 08 2002 09:10 AM (54319 seconds)
      Prefix: 3FFE:C00:C18:2::/72
        preferred lifetime 300, valid lifetime 54333
        expires at Nov 08 2002 09:11 AM (54331 seconds)
      Prefix: 3FFE:C00:C18:3::/72
        preferred lifetime 280, valid lifetime 51111
        expires at Nov 08 2002 08:17 AM (51109 seconds)
    DNS server: 1001::1
  
```

show ipv6 dhcp interface

```

DNS server: 1001::2
Domain name: domain1.net
Domain name: domain2.net
Domain name: domain3.net
Prefix name is cli-p1
Rapid-Commit is enabled

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 34: show ipv6 dhcp interface フィールドの説明

フィールド	説明
Ethernet2/1 is in server/client mode	指定したインターフェイスがサーバモードまたはクライアントモードのいずれであるかを表示します。
Preference value:	指定したサーバのアドバタイズされた（またはデフォルトの 0 の）プリファレンス値。
Prefix name is cli-p1	このインターフェイス上で正常に取得したプレフィックスを格納する IPv6 汎用プレフィックス プール名を表示します。
Using pool: svr-p1	インターフェイスが使用しているプールの名前。
State is OPEN	このインターフェイス上の DHCP for IPv6 クライアントの状態。「Open」は、設定情報を受信したことを示します。
List of known servers	インターフェイス上のサーバのリストを表示します。
Address, DUID	指定したインターフェイス上で聴取したサーバのアドレスと DHCP 固有識別子 (DUID)。
Rapid commit is disabled	rapid-commit キーワードがインターフェイス上で有効になっているかどうかを表示します。

次に、FastEthernet インターフェイス 0/0 上の DHCP for IPv6 リレーエージェントの設定と **show ipv6 dhcp interface** コマンドを使用した FastEthernet インターフェイス 0/0 上のリレーエージェント情報の表示の例を示します。

```

デバイス(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
デバイス# show ipv6 dhcp interface FastEthernet 0/0
FastEthernet0/0 is in relay mode
Relay destinations:
FE80::250:A2FF:FEBF:A056 via FastEthernet0/1

```

Related Commands

Command	Description
ipv6 dhcp client pd	DHCP for IPv6 クライアントプロセスを有効にし、指定したインターフェイスを通じてプレフィックス委任の要求を有効にします。

Command	Description
ipv6 dhcp relay destination	クライアントメッセージを転送する宛先アドレスを指定し、インターフェイスで DHCP for IPv6 リレー サービスを有効にします。
ipv6 dhcp server	インターフェイス上で DHCP for IPv6 サービスを有効にします。

show ipv6 dhcp relay binding

DHCPv6 Internet Assigned Numbers Authority (IANA) と DHCPv6 Identity Association for Prefix Delegation (IAPD) のリレーエージェント上でのバインディングを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 dhcp relay binding** コマンドを使用します。

show ipv6 dhcp relay binding [*vrf vrf-name*]

Syntax Description	vrf <i>vrf-name</i> (任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
Command Modes	ユーザ EXEC (>) 特権 EXEC (#)
Command History	
Command History	リリース
	変更内容
	Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。
Usage Guidelines	vrf <i>vrf-name</i> キーワードと引数のペアを指定すると、指定した VRF に属するすべてのバインディングが表示されます。



Note リレーエージェント上の DHCPv6 IAPD バインディングは、Cisco uBR10012 および Cisco uBR7200 シリーズのユニバーサルブロードバンドデバイス上に表示されます。

Examples

次に、**show ipv6 dhcp relay binding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp relay binding
```

次に、Cisco uBR10012 ユニバーサルブロードバンドデバイス上に指定した VRF 名を使用した **show ipv6 dhcp relay binding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp relay binding vrf vrf1
```

```
Prefix: 2001:DB8:0:1:/64 (Bundle100.600)
DUID: 000300010023BED94D31
IAID: 3201912114
lifetime: 600
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 35: show ipv6 dhcp relay binding フィールドの説明

フィールド	説明
Prefix	DHCP の IPv6 プレフィックス。
DUID	IPv6 リレーバインディングの DHCP 固有識別子 (DUID)。
IAID	DHCP のアイデンティティ関連付け識別 (IAID)。
lifetime	プレフィックスのライフタイム (秒単位)。

Related Commands

コマンド	説明
clear ipv6 dhcp relay binding	IPv6 リレーバインディングの DHCP の特定の IPv6 アドレスまたは IPv6 プレフィックスをクリアします。
debug ipv6 dhcp relay	IPv6 DHCP リレーエージェントのデバッグをイネーブルにします。
debug ipv6 dhcp relay bulk-lease	IPv6 DHCP リレーエージェントの bulk lease クエリのデバッグをイネーブルにします。

show ipv6 eigrp events

IPv6 について記録された Enhanced Interior Gateway Routing Protocol (EIGRP) イベントを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 eigrp events** コマンドを使用します。

show ipv6 eigrp events [[errmsg | sia] [event-num-start event-num-end] | type]

Syntax Description	Parameter	Description
	errmsg	(任意) ログに記録されているエラーメッセージを表示します。
	sia	(任意) Stuck In Active (SIA) メッセージを表示します。
	event-num-start	(任意) イベントの範囲の開始番号。範囲は 1 ~ 4294967295 です。
	event-num-end	(任意) イベントの範囲の終了番号。範囲は 1 ~ 4294967295 です。
	type	(任意) ログに記録されているイベントタイプを表示します。

Command Default イベントの範囲を指定しないと、IPv6 EIGRP のすべてのイベントに関する情報が表示されます。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	Release	Change Content
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ipv6 eigrp events** コマンドは、シスコサポートチームがネットワーク障害の分析に使用します。一般的な使用は意図していません。このコマンドは、EIGRP に関する内部状態情報と、ルート通知と変更の処理方法を表示します。

Examples 次に、**show ipv6 eigrp events** コマンドの出力例を示します。フィールドの説明は自明です。

```

デバイス# show ipv6 eigrp events
Event information for AS 65535:
1 00:56:41.719 State change: Successor Origin Local origin
2 00:56:41.719 Metric set: 2555:5555::/32 4294967295
3 00:56:41.719 Poison squashed: 2555:5555::/32 lost if
4 00:56:41.719 Poison squashed: 2555:5555::/32 rt gone
5 00:56:41.719 Route installing: 2555:5555::/32 FE80::ABCD:4:EF00:1
6 00:56:41.719 RDB delete: 2555:5555::/32 FE80::ABCD:4:EF00:2
7 00:56:41.719 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:1
8 00:56:41.719 Find FS: 2555:5555::/32 4294967295
9 00:56:41.719 Free reply status: 2555:5555::/32
10 00:56:41.719 Clr handle num/bits: 0 0x0
11 00:56:41.719 Clr handle dest/cnt: 2555:5555::/32 0

```

```

12 00:56:41.719 Rcv reply met/succ met: 4294967295 4294967295
13 00:56:41.719 Rcv reply dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
14 00:56:41.687 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:2
15 00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
16 00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
17 00:56:41.687 State change: Local origin Successor Origin
18 00:56:41.687 Metric set: 2555:5555::/32 4294967295
19 00:56:41.687 Active net/peers: 2555:5555::/32 65536
20 00:56:41.687 FC not sat Dmin/met: 4294967295 2588160
21 00:56:41.687 Find FS: 2555:5555::/32 2588160
22 00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
23 00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:1
24 00:56:41.659 Change queue emptied, entries: 1
25 00:56:41.659 Metric set: 2555:5555::/32 2588160

```

Related Commands

コマンド	説明
clear ipv6 eigrp	EIGRP for IPv6 ルーティングテーブルからエントリを削除します。
debug ipv6 eigrp	IPv6 プロトコル用の EIGRP に関する情報を表示します。
ipv6 eigrp	指定したインターフェイスで EIGRP for IPv6 を有効にします。

show ipv6 eigrp interfaces

IPv6 トポロジで Enhanced Interior Gateway Routing Protocol (EIGRP) に設定されているインターフェイスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 eigrp interfaces** コマンドを使用します。

show ipv6 eigrp [*as-number*] **interfaces** [*type number*] [**detail**]

Syntax Description

<i>as-number</i>	(任意) 自律システム番号。
<i>type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>number</i>	(任意) インターフェイス番号。ネットワークングデバイスに対する番号付け構文の詳細については、疑問符 (?) のオンラインヘルプ機能を使用してください。
detail	(任意) インターフェイスの詳細情報を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

EIGRP がアクティブになっているインターフェイスを特定し、それらのインターフェイスに関連する EIGRP プロセスの情報を取得するには、**show ipv6 eigrp interfaces** コマンドを使用します。オプションの *type number* 引数と **detail** キーワードは任意の順序で入力できます。

インターフェイスが指定された場合、そのインターフェイスのみが表示されます。指定されない場合、EIGRP を実行しているすべてのインターフェイスが表示されます。

自律システムが指定された場合、指定された自律システムについてのルーティングプロセスのみが表示されます。指定されない場合、すべての EIGRP プロセスが表示されます。

Examples

次に、**show ipv6 eigrp interfaces** コマンドの出力例を示します。

```
デバイス# show ipv6 eigrp 1 interfaces
```

```
IPv6-EIGRP interfaces for process 1
Interface      Peers    Xmit Queue  Mean    Pacing Time  Multicast    Pending
                Un/Reliable SRTT      Un/Reliable Flow Timer   Routes
Et0/0          0        0/0         0       0/10         0            0
```

次に、**show ipv6 eigrp interfaces detail** コマンドの出力例を示します。

デバイス# **show ipv6 eigrp interfaces detail**

```
IPv6-EIGRP interfaces for process 1
          Xmit Queue   Mean      Pacing Time   Multicast      Pending
Interface  Peers  Un/Reliable  SRTT      Un/Reliable   Flow Timer     Routes
Et0/0      0      0/0         0         0/10         0              0
Hello interval is 5 sec
Next xmit serial <none>
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Authentication mode is not set
```

次に、**no ipv6 next-hop self** コマンドを **no-ecmp-mode** オプションを指定して設定した特定のインターフェイスに関する詳細情報を表示する **show ipv6 eigrp interface detail** コマンドの出力例を示します。

Deviceデバイス# **show ipv6 eigrp interfaces detail tunnel 0**

```
EIGRP-IPv6 Interfaces for AS(1)
          Xmit Queue   PeerQ      Mean      Pacing Time   Multicast      Pending
Interface  Peers  Un/Reliable  Un/Reliable SRTT      Un/Reliable   Flow Timer     Routes
Tu0/0      2      0/0         0/0         29       0/0          136            0
Hello-interval is 5, Hold-time is 15
  Split-horizon is disabled
  Next xmit serial <none>
  Packetized sent/expedited: 48/1
  Hello's sent/expedited: 13119/49
  Un/reliable mcasts: 0/20 Un/reliable ucasts: 31/398
  Mcast exceptions: 5 CR packets: 5 ACKs suppressed: 1
  Retransmissions sent: 355 Out-of-sequence rcvd: 6
  Next-hop-self disabled, next-hop info forwarded, ECMP mode Enabled
  Topology-ids on interface - 0
  Authentication mode is not set
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 36: show ipv6 eigrp interfaces フィールドの説明

フィールド	説明
Interface	EIGRP が設定されているインターフェイス。
Peers	直接接続された EIGRP ネイバーの数。
Xmit Queue Un/Reliable	信頼性の低い送信キューおよび信頼性の高い送信キューに残っているパケットの数。
Mean SRTT	平均スムーズ ラウンドトリップ時間 (SRTT) 間隔 (秒単位)。
Pacing Time Un/Reliable	インターフェイスから EIGRP パケット (信頼性の低いパケットおよび信頼性の高いパケット) を送信するタイミングを決定するために使用するペーシング時間 (秒単位)。
Multicast Flow Timer	デバイスがマルチキャスト EIGRP パケットを送信する最大秒数。

フィールド	説明
Pending Routes	送信キュー内で送信を待機しているルートの数。
Hello interval is 5 sec	hello 間隔の時間（秒単位）。

show ipv6 eigrp topology

Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 トポロジテーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 eigrp topology** コマンドを使用します。

show ipv6 eigrp topology [*as-number ipv6-address*] [**active** | **all-links** | **pending** | **summary** | **zero-successors**]

Syntax Description	
<i>as-number</i>	(任意) 自律システム番号。
<i>ipv6-address</i>	(任意) IPv6 アドレス。
active	(任意) EIGRP トポロジテーブル内のアクティブ エントリのみ表示します。
all-links	(任意) (到達不能な後継ソースを含む) EIGRP トポロジテーブル内の全エントリを表示します。
pending	(任意) ネイバーからのアップデートを待機しているか、ネイバーへの応答を待機している、EIGRP トポロジテーブル内のすべてのエントリを表示します。
summary	(任意) EIGRP トポロジテーブルの要約を表示します。
zero-successors	(任意) サクセサがない利用可能なルートを表示します。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドがキーワードや引数なしで使用される場合、到達可能な後継ルータのルートだけが表示されます。**show ipv6 eigrp topology** コマンドを使用すると、Diffusing Update Algorithm (DUAL) の状態を判断し、起こり得る DUAL の問題をデバッグできます。

Examples

次に、**show ipv6 eigrp topology** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```
デバイス# show ipv6 eigrp topology
```

```
IPv6-EIGRP Topology Table for AS(1)/ID(2001:0DB8:10::/64)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
```

show ipv6 eigrp topology

```
P 2001:0DB8:3::/64, 1 successors, FD is 281600
via Connected, Ethernet1/0
```

次に、EIGRP トポロジに **no-ecmp-mode** を指定せずに **no ipv6 next-hop-self** コマンドを設定した場合に ECMP モード情報を表示する **show ipv6 eigrp topology prefix** コマンドの出力例を示します。ECMP モードは、アドバタイズされているパスに関する情報を提供しません。複数のサクセサが存在する場合、一番上のパスがすべてのインターフェイス上のデフォルトパスとしてアドバタイズされ、出力に「ECMP Mode: Advertise by default」というメッセージが表示されます。デフォルトパス以外のパスがアドバタイズされる場合は、「ECMP Mode: Advertise out <Interface name>」というメッセージが表示されます。出力にはフィールドの説明も表示されます。

```
デバイス# show ipv6 eigrp topology 2001:DB8:10::1/128
```

```
EIGRP-IPv6 Topology Entry for AS(1)/ID(192.0.2.100) for 2001:DB8:10::1/128
State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
Descriptor Blocks:
FE80::A8BB:CCFF:FE01:2E01 (Tunnel0), from FE80::A8BB:CCFF:FE01:2E01, Send flag is 0x0
Composite metric is (284160/281600), route is Internal
Vector metric:
  Minimum bandwidth is 10000 Kbit
  Total delay is 1100 microseconds
  Reliability is 255/255
  Load is 1/5
  Minimum MTU is 1400
  Hop count is 1
  Originating router is 10.10.1.1
ECMP Mode: Advertise by default
FE80::A8BB:CCFF:FE01:3E01 (Tunnel1), from FE80::A8BB:CCFF:FE01:3E01, Send flag is 0x0
Composite metric is (284160/281600), route is Internal
Vector metric:
  Minimum bandwidth is 10000 Kbit
  Total delay is 1100 microseconds
  Reliability is 255/255
  Load is 1/5
  Minimum MTU is 1400
  Hop count is 1
  Originating router is 10.10.2.2
ECMP Mode: Advertise out Tunnel1
```

Related Commands

コマンド	説明
show eigrp address-family topology	EIGRP トポロジテーブル内のエントリを表示します。

show ipv6 eigrp traffic

送受信される Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 のパケットを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 eigrp traffic** コマンドを使用します。

show ipv6 eigrp traffic [*as-number*]

Syntax Description

<i>as-number</i>	(任意) 自律システム番号。
------------------	----------------

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

送受信されるパケットの情報を表示するには、**show ipv6 eigrp traffic** コマンドを使用します。

Examples

次に、**show ipv6 eigrp traffic** コマンドの出力例を示します。

```

デバイス# show ipv6 eigrp traffic
IPv6-EIGRP Traffic Statistics for process 9
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 37: show ipv6 eigrp traffic フィールドの説明

フィールド	説明
process 9	ipv6 router eigrp コマンドで指定された自律システム (AS) 番号
Hellos sent/received	送受信された hello パケットの数
Updates sent/received	送受信されたアップデート パケットの数
Queries sent/received	送受信されたクエリー パケットの数
Replies sent/received	送受信された応答パケットの数
Acks sent/received	送受信された確認応答 (ACK) パケットの数

show ipv6 eigrp traffic**Related Commands**

コマンド	説明
ipv6 router eigrp	EIGRP for IPv6 ルーティング プロセスを設定します。

show ipv6 general-prefix

IPv6 の汎用プレフィックスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 general-prefix** コマンドを使用します。

show ipv6 general-prefix

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IPv6 の汎用プレフィックスに関する情報を表示するには、**show ipv6 general-prefix** コマンドを使用します。

Examples

次に、6to4 に基づいて定義された **my-prefix** という IPv6 汎用プレフィックスの例を示します。また、汎用プレフィックスは、インターフェイス **loopback42** 上にアドレスを定義するためにも使用します。

```

デバイス# show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
  Loopback42 (Address command)

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 38: show ipv6 general-prefix フィールドの説明

フィールド	説明
IPv6 Prefix	IPv6 汎用プレフィックスのユーザ定義名。
Acquired via	汎用プレフィックスは 6to4 インターフェイスに基づいて定義されています。また、汎用プレフィックスは手動で定義するか、または IPv6 プレフィックス委任の DHCP を使用して取得することもできます。
2002:B0B:B0B::/48	この汎用プレフィックスのプレフィックス値。
Loopback42 (Address コマンド)	この汎用プレフィックスを使用するインターフェイスのリスト。

show ipv6 general-prefix**Related Commands**

Command	Description
ipv6 general-prefix	IPv6 アドレスの汎用プレフィックスを手動で定義します。

show ipv6 interface

IPv6 に設定したインターフェイスのユーザビリティステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 interface** コマンドを使用します。

show ipv6 interface [**brief**][*type number*][**prefix**]

Syntax Description	
brief	(任意) 各インターフェイスの IPv6 ステータスおよび設定の簡単なサマリーを表示します。
<i>type</i>	(任意) 情報を表示するインターフェイス タイプ。
<i>number</i>	(任意) 情報を表示するインターフェイス番号。
prefix	(任意) ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。

Command Default すべての IPv6 インターフェイスが表示されます。

Command Modes ユーザ EXEC (>)

特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ipv6 interface** コマンドは、IPv6 に固有であることを除き、**show ip interface** コマンドと同様です。

show ipv6 interface コマンドを使用して、インターフェイスの IPv6 ステータスと設定されたアドレスを検証します。また、**show ipv6 interface** コマンドは、このインターフェイスおよび設定されている機能の動作に IPv6 が使用しているパラメータも表示します。

インターフェイスのハードウェアが使用できる場合、インターフェイスは **up** とマークされます。インターフェイスが双方向通信を IPv6 に提供できる場合、回線プロトコルのステータスは **up** とマークされます。

オプションのインターフェイス タイプと番号を指定すると、このコマンドはその特定のインターフェイスに関する情報のみを表示します。特定のインターフェイスについて、インターフェイスに設定されている IPv6 ネイバー探索 (ND) プレフィックスを表示するには、**prefix** キーワードを使用します。

IPv6 が設定された特定のインターフェイスに関するインターフェイス情報

show ipv6 interface コマンドは、指定されたインターフェイスに関する情報を表示します。

```

デバイス(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
No Virtual link-local address(es):
Global unicast address(es):
  2001::1, subnet is 2001::/64 [DUP]
  2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
  2001:100::1, subnet is 2001:100::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
  FF02::1:FF00:6700
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 39: show ipv6 interface フィールドの説明

フィールド	説明
Ethernet0/0 is up, line protocol is up	インターフェイスハードウェアがアクティブかどうか（回線信号が存在するかどうか）と、それが管理者によりダウン状態にされているかどうかを示します。インターフェイスのハードウェアが使用できる場合、インターフェイスは up とマークされます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。
line protocol is up, down（出力例に down は表示されていません）	回線プロトコルを処理するソフトウェアプロセスが回線を使用可能と見なしているかどうか（つまり、キープアライブが成功しているかどうか、または IPv6 CP がネゴシエートされているかどうか）を示します。インターフェイスが双方向通信を提供できる場合、回線プロトコルは up とマークされます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。

フィールド	説明
IPv6 is enabled, stalled, disabled (出力例には stalled と disabled は表示されていません)	IPv6がインターフェイスでイネーブル、ストールまたはディセーブルかを示します。IPv6が有効になっている場合は、インターフェイスのステータスが「enabled」と表示されます。重複アドレス検出でインターフェイスのリンクローカルアドレスが重複していると特定された場合は、そのインターフェイスでのIPv6パケットの処理が無効になり、インターフェイスのステータスが「stalled」になります。IPv6が有効になっていない場合は、インターフェイスのステータスが「disabled」と表示されます。
link-local address	インターフェイスに割り当てられているリンクローカルアドレスを表示します。
Global unicast address(es):	インターフェイスに割り当てられているグローバルユニキャストアドレスを表示します。
Joined group address(es):	インターフェイスが属するマルチキャストグループを示します。
MTU	インターフェイスの最大伝送単位。
ICMP error messages	このインターフェイスで送信されるエラーメッセージ間の最小間隔（ミリ秒単位）を指定します。
ICMP redirects	インターフェイスでの Internet Control Message Protocol (ICMP) IPv6 リダイレクトメッセージの状態（メッセージの送信が有効か無効か）。
ND DAD	インターフェイスでの重複アドレス検出の状態（enabled または disabled）。
number of DAD attempts:	重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー送信要求メッセージの連続数。
ND reachable time	このインターフェイスに割り当てられているネイバー探索到達可能時間（ミリ秒）を表示します。
ND advertised reachable time	このインターフェイスでアドバタイズされるネイバー探索到達可能時間（ミリ秒）を表示します。
ND advertised retransmit interval	このインターフェイスでアドバタイズされるネイバー探索再送信間隔（ミリ秒）を表示します。

フィールド	説明
ND router advertisements	このインターフェイスで送信されるネイバー探索ルータアドバタイズメント (RA) の間隔 (秒単位) およびアドバタイズメントが期限切れになるまでの時間数を指定します。 Cisco IOS Release 12.4(2)T 現在、このフィールドには、このインターフェイス上のこのデバイスが送信したデフォルトのルータ設定が表示されます。
ND advertised default router preference is Medium	特定のインターフェイス上のデバイスの DRP。

show ipv6 interface コマンドは、インターフェイスに割り当てられている IPv6 アドレスと関連付けられている可能性がある属性に関する情報を表示します。

属性	説明
ANY	エニーキャスト。アドレスは ipv6 address コマンドを使用して設定した時点で指定したとおりのエニーキャストアドレスです。
CAL	カレンダー。アドレスには時間制限が設定されており、有効な優先期間があります。
DEP	非推奨。時限アドレスは推奨されません。
DUP	重複。アドレスは、重複アドレス検出 (DAD) によって決定されたとおりの重複しています。DAD を再試行するには、 shutdown または no shutdown コマンドをインターフェイス上で実行する必要があります。
EUI	EUI-64 ベース。アドレスは EUI-64 を使用して生成されました。
OFF	オフリンク。アドレスはオフリンクです。
OOD	過度に楽観的な DAD。このアドレスに対して DAD は実行されません。この属性は仮想アドレスに適用されます。
PRE	優先時限アドレスが優先されます。
TEN	暫定。アドレスは DAD により暫定的な状態になっています。

属性	説明
UNA	アクティブ化されていません。仮想アドレスはアクティブになっておらず、スタンバイ状態です。
VIRT	仮想。アドレスは仮想であり、HSRP、VRRP、または GLBP によって管理されます。

brief キーワードを使用した show ipv6 interface コマンド

次に、**brief** キーワードを使用して入力した場合の **show ipv6 interface** コマンドの出力例を示します。

```

デバイス# show ipv6 interface brief
Ethernet0 is up, line protocol is up
Ethernet0          [up/up]
    unassigned
Ethernet1          [up/up]
    2001:0DB8:1000:/29
Ethernet2          [up/up]
    2001:0DB8:2000:/29
Ethernet3          [up/up]
    2001:0DB8:3000:/29
Ethernet4          [up/down]
    2001:0DB8:4000:/29
Ethernet5          [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8
Interface          Status          IPv6 Address
Ethernet0          up              3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1          up              unassigned
Fddi0              up              3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0            administratively down unassigned
Serial1            administratively down unassigned
Serial2            administratively down unassigned
Serial3            administratively down unassigned
Tunnel0            up              unnumbered (Ethernet0)
Tunnel1            up              3FFE:700:20:1::12

```

ND プレフィックスを設定した IPv6 インターフェイス

次に、ローカル IPv6 プレフィックス プールからプレフィックスを生成したインターフェイスの特性の出力例を示します。

```

デバイス# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
  ipv6 address 2001:0DB8::1/64
  ipv6 address 2001:0DB8::2/64
  ipv6 nd prefix 2001:0DB8:2::/64
  ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.

```

```
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar
       default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD    2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD   2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P     2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800
```

デフォルトのプレフィックスでは、`ipv6 nd prefix default` コマンドを使用して設定したパラメータを表示します。

DRP を設定した IPv6 インターフェイス

次に、インターフェイスを通じてこのデバイスがアドバタイズした DRP プリファレンス値の状態の出力例を示します。

```
デバイス# show ipv6 interface gigabitethernet 0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::130
Description: Management network (dual stack)
Global unicast address(es):
  FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:130
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Low
Hosts use stateless autoconfig for addresses.
```

HSRP が設定された IPv6 インターフェイス

最初に HSRP IPv6 をインターフェイス上に設定すると、インターフェイス IPv6 リンクローカルアドレスは非アクティブ (UNA) とマークされます。これは、アドバタイズされることがなく、HSRP IPv6 仮想リンクローカルアドレスが UNA 属性および暫定 DAD (TEN) 属性が設定された仮想リンクローカルアドレスリストに追加されるためです。また、インターフェイスも HSRP IPv6 マルチキャストアドレスをリッスンするようにプログラミングされます。

次に、HSRP IPv6 がインターフェイス上に設定されている場合の UNA 属性と TEN 属性のステータスの出力例を示します。

```
デバイス# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80:2::2 [UNA]
```

```

Virtual link-local address(es):
  FE80::205:73FF:FEA0:1 [UNA/TEN]
Global unicast address(es):
  2001:2::2, subnet is 2001:2::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::66
  FF02::1:FF00:2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ND DAD is enabled, number of DAD attempts: 1

```

HSRP グループがアクティブになると UNA 属性と TEN 属性がクリアされ、過度に楽観的な DAD (OOD) 属性が設定されます。HSRP 仮想 IPv6 アドレスの要請ノードマルチキャストアドレスもインターフェイスに追加されます。

次に、HSRP グループがアクティブになっている場合の UNA 属性、TEN 属性、および OOD 属性のステータスの出力例を示します。

```

# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80:2::2 [UNA]
Virtual link-local address(es):
  FE80::205:73FF:FEA0:1 [OPT]
Global unicast address(es):
  2001:2::2, subnet is 2001:2::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::66
  FF02::1:FF00:2
  FF02::1:FFA0:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1

```

次の表で、HSRP を設定した **show ipv6 interface** コマンドの表示に示された追加の重要フィールドについて説明します。

Table 40: HSRP を設定した show ipv6 interface コマンドのフィールドの説明

フィールド	説明
IPv6 is enabled, link-local address is FE80:2::2 [UNA]	インターフェイス IPv6 リンクローカルアドレスは、アドレスがバタイズされないため、UNA とマークされます。
FE80::205:73FF:FEA0:1 [UNA/TEN]	UNA 属性と TEN 属性が設定された仮想リンクローカルアドレスリスト。
FF02::66	HSRP IPv6 マルチキャストアドレス。
FE80::205:73FF:FEA0:1 [OPT]	HSRP がアクティブになり、HSRP 仮想アドレスは OPT とマークされます。
FF02::1:FFA0:1	HSRP 要請ノードマルチキャストアドレス。

最小 RA 間隔が設定された IPv6 インターフェイス

インターフェイス上でモバイル IPv6 を有効にすると、IPv6 ルータ アドバタイズメント (RA) 伝送間の最小間隔を設定できます。show ipv6 interface コマンドの出力には、最小 RA 間隔が設定されていれば、その間隔が報告されます。最小 RA 間隔が明示的に設定されていない場合は表示されません。

次の例では、イーサネット インターフェイス 1/0 上で最大 RA 間隔は 100 秒、最小 RA 間隔は 60 秒に設定されています。

```
デバイス(config-if)# ipv6 nd ra-interval 100 60
```

その後で show ipv6 interface を使用すると、間隔が次のように表示されます。

```
デバイス(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachable are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

次の例では、イーサネット インターフェイス 1/0 上で最大 RA 間隔は 100 ミリ秒 (ms)、最小 RA 間隔は 60 ms に設定されています。

```
デバイス(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachable are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 milliseconds
  ND router advertisements live for 1800 seconds
```

```
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

次の表で、最小 RA 間隔情報を設定した **show ipv6 interface** コマンドの表示に示された追加の重要フィールドについて説明します。

Table 41: 最小 RA 間隔情報を設定した **show ipv6 interface** コマンドのフィールドの説明

フィールド	説明
ND router advertisements are sent every 60 to 100 seconds	最小値と最大値の間の値からランダムに選択した間隔で ND RA が送信されます。次の例では、最小値は 60 秒、最大値は 100 秒です。
ND router advertisements are sent every 60 to 100 milliseconds	最小値と最大値の間の値からランダムに選択した間隔で ND RA が送信されます。次の例では、最小値は 60 ミリ秒、最大値は 100 ミリ秒です。

Related Commands

コマンド	説明
ipv6 nd prefix	IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。
ipv6 nd ra interval	インターフェイス上の IPv6 RA 送信間隔を設定します。
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

show ipv6 mfib

IPv6 マルチキャスト転送情報ベース (MFIB) 内の転送エントリとインターフェイスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mfib** コマンドを使用します。

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope** | **verbose** *group-address-name* | *ipv6-prefix/ prefix-length* | *source-address-name* | **interface** | **status** | **summary**]

show ipv6 mfib [**vrf** *vrf-name*] [**all** | **linkscope** | **verbose** | **interface** | **status** | **summary**]

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
all	(任意) IPv6 MFIB 内のすべての転送エントリとインターフェイスを表示します。
linkscope	(任意) リンク ローカル グループを表示します。
verbose	(任意) MAC カプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報を表示します。
<i>ipv6-prefix</i>	(任意) インターフェイスに割り当てられた IPv6 ネットワーク。デフォルトの IPv6 プレフィックスは 128 です。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>/ prefix-length</i>	(オプション) IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
<i>group-address-name</i>	(任意) マルチキャスト グループの IPv6 アドレスまたは名前。
<i>source-address-name</i>	(任意) マルチキャスト グループの IPv6 アドレスまたは名前。
interface	(任意) インターフェイスの設定とステータス。
status	(任意) 一般的な設定とステータス。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

MFIBのエントリと転送インターフェイスおよびそれらのトラフィック統計を表示するには、**show ipv6 mfib** コマンドを使用します。ルータが分散モードで動作している場合、仮想 IP (VIP) 上でこのコマンドをイネーブルにできます。

MFIBの転送エントリには、転送とシグナリングのデフォルト動作を決定するフラグがあり、エントリに一致するパケットで使用されます。エントリにはインターフェイス単位のフラグもあり、特定のインターフェイスで受信または転送されるパケットについての転送動作をさらに詳しく指定します。次の表に、MFIB 転送エントリとインターフェイス フラグを示します。

Table 42: MFIB エントリとインターフェイスのフラグ

フラグ	説明
F	Forward: データは、このインターフェイスから転送されます。
A	Accept: このインターフェイス上で受信されたデータは、転送用として受け入れられます。
IC	Internal copy: このインターフェイスで受信または転送されたパケットのコピーをルータに配信します。
NS	Negate signal: このインターフェイスで受信されたパケットについては、デフォルトのエントリ シグナリング動作を逆にします。
DP	Do not preserve: このインターフェイスでのパケット受信を信号で通知するときに、コピーを保存しません (破棄します)。
SP	Signal present: このインターフェイスでのパケットの受信が信号で通知されました。
S	Signal: デフォルトでは、このエントリに一致するパケットの受信を信号で通知します。
C	このエントリに一致するパケットについて、直接接続チェックを実行します。パケットが、直接接続されている送信元から発信されていた場合は、受信を信号で通知します。

Examples

次に、MFIBでの転送エントリおよびインターフェイスを表示する例を示します。ルータは高速スイッチング用に設定されており、受信側はイーサネット 1/1 の FF05::1 に加入し、送信元 (2001::1:1:20) はイーサネット 1/2 で送信しています。

```

デバイス# show ipv6 mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
              AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                 IC - Internal Copy, NP - Not platform switched
                 SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
Forwarding: 0/0/0/0, Other: 0/0/0

```

```

Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::/1) Flags: C
  Forwarding: 2/0/100/0, Other: 0/0/0
  Tunnel0 Flags: A NS
  Ethernet1/1 Flags: F NS
    Pkts: 0/2
(2001::1:1:200,FF05::/1) Flags:
  Forwarding: 5/0/100/0, Other: 0/0/0
  Ethernet1/2 Flags: A
  Ethernet1/1 Flags: F NS
    Pkts: 3/2
(*,FF10::/15) Flags: D
  Forwarding: 0/0/0/0, Other: 0/0/0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 43: show ipv6 mfib フィールドの説明

フィールド	説明
Entry Flags	エントリーに関する情報です。
Forwarding Counts	少なくとも1つのインターフェイスから受信され、少なくとも1つのインターフェイスに転送されたパケットに関する統計。
Pkt Count/	このカウンタが適用されるマルチキャスト転送状態の作成後に受信され転送されたパケットの総数。
Pkts per second/	1秒間に受信され転送されたパケット数。
Avg Pkt Size/	このマルチキャスト転送状態についての合計バイト数/合計パケット数。合計バイト数は直接は表示されません。平均パケットサイズにパケット数を乗算すると、合計バイト数を計算できます。
Kbits per second	1秒間のバイト数/1秒間のパケット数/1000。
Other counts:	受信パケットに関する統計。これらのカウンタには、受信され転送されたパケットと受信されても転送されなかったパケットに関する統計が含まれます。
Interface Flags:	インターフェイスに関する情報。
Interface Counts:	インターフェイス統計情報。

次に、グループアドレスに FF03:1::1 を指定した MFIB 内の転送エントリーとインターフェイスの例を示します。

```

デバイス# show ipv6 mfib FF03:1::1
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A
flag,
          AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
second

```

```

Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
*,FF03:1::1) Flags:C
  Forwarding:0/0/0/0, Other:0/0/0
  Tunnel1 Flags:A NS
  GigabitEthernet5/0.25 Flags:F NS
    Pkts:0/0
  GigabitEthernet5/0.24 Flags:F NS
    Pkts:0/0
(5002:1::2,FF03:1::1) Flags:
  Forwarding:71505/0/50/0, Other:42/0/42
  GigabitEthernet5/0 Flags:A
  GigabitEthernet5/0.19 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.20 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.21 Flags:F NS
    Pkts:238/24
.
.
.
GigabitEthernet5/0.16 Flags:F NS
Pkts:71628/24

```

次に、グループアドレス FF03:1::1、送信元アドレス 5002:1::2 を指定した MFIB 内の転送エントリとインターフェイスの例を示します。

```

デバイス# show ipv6 mfib FF03:1::1 5002:1::2

```

```

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
              AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(5002:1::2,FF03:1::1) Flags:
  Forwarding:71505/0/50/0, Other:42/0/42
  GigabitEthernet5/0 Flags:A
  GigabitEthernet5/0.19 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.20 Flags:F NS
    Pkts:239/24
.
.
.
  GigabitEthernet5/0.16 Flags:F NS
    Pkts:71628/24

```

次に、グループアドレス FF03:1::1 とデフォルトプレフィックス 128 を指定した MFIB 内の転送エントリとインターフェイスの例を示します。

```

デバイス# show ipv6 mfib FF03:1::1/128

```

```

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
              AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

```

```

Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FF03::1) Flags:C
  Forwarding:0/0/0/0, Other:0/0/0
  Tunnel1 Flags:A NS
  GigabitEthernet5/0.25 Flags:F NS
    Pkts:0/0
  GigabitEthernet5/0.24 Flags:F NS
    Pkts:0/0
.
.
.
  GigabitEthernet5/0.16 Flags:F NS
    Pkts:0/0

```

次に、グループアドレス FFE0 とプレフィックス 15 を指定した MFIB 内の転送エントリとインターフェイスの例を示します。

```

デバイス# show ipv6 mfib FFE0::/15
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FFE0::/15) Flags:D
  Forwarding:0/0/0/0, Other:0/0/0

```

次に、**show ipv6 mfib** コマンドで **verbose** キーワードを指定した場合の出力例を示します。ここでは、MFIB 内の転送エントリおよびインターフェイスと、MAC カプセル化ヘッダーやプラットフォーム固有情報などの追加情報が表示されます。

```

デバイス# show ipv6 mfib ff33::1:1 verbose
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry, HB - Bridge entry, HD - NonRPF Drop entry,
                NP - Not platform switchable, RPL - RPF-ltl linkage,
                MCG - Metset change, ERR - S/w Error Flag, RTY - In RetryQ,
                LP - L3 pending, MP - Met pending, AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                IC - Internal Copy, NP - Not platform switched
                SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(10::2,FF33::1:1) Flags: K
  RP Forwarding: 0/0/0/0, Other: 0/0/0
  LC Forwarding: 0/0/0/0, Other: 0/0/0
  HW Forwd: 0/0/0/0, Other: NA/NA/NA
  Slot 6: HW Forwarding: 0/0, Platform Flags: HF RPL
  Slot 1: HW Forwarding: 0/0, Platform Flags: HF RPL
  Vlan10 Flags: A

```

```
Vlan30 Flags: F NS
Pkts: 0/0/0 MAC: 33330001000100D0FFFE180086DD
```

次の表に、この出力で表示されるフィールドについて説明します。

Table 44: show ipv6 mfib verbose フィールドの説明

フィールド	説明
Platform flags	プラットフォームに関する情報
Platform per slot HW-Forwarding Counts	転送されたバイトあたりのパケット総数

Related Commands

コマンド	説明
show ipv6 mfib active	アクティブな送信元からマルチキャストグループへの送信レートを表示します。
show ipv6 mfib count	MFIB からのグループおよび送信元に関するサマリートラフィック統計情報を表示します。
show ipv6 mfib interface	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
show ipv6 mfib status	一般的な MFIB 設定と動作ステータスを表示します。
show ipv6 mfib summary	IPv6 MFIB エントリ（リンクローカルグループを含む）およびインターフェイスの数に関するサマリー情報を表示します。

show ipv6 mld groups

ルータに直接接続されたマルチキャストグループと、マルチキャストリスナー検出（MLD）を通じて学習したマルチキャストグループを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mld groups** コマンドを使用します。

show ipv6 mld [**vrf** *vrf-name*] **groups** [**link-local**] [*group-name**group-address*] [*interface-type* *interface-number*] [**detail** | **explicit**]

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
link-local	(任意) リンク ローカル グループを表示します。
<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。
<i>interface-type</i> <i>interface-number</i>	(任意) インターフェイス タイプおよび番号
detail	(任意) 個々の送信元の詳細情報を表示します。
explicit	(任意) 各グループの各インターフェイスで明示的に追跡しているホストに関する情報を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

オプションの引数をすべて省略すると、**show ipv6 mld groups** コマンドは、グループアドレス別およびインターフェイスタイプと番号別に直接接続されたすべてのマルチキャストグループを表示します。これには、使用したリンクローカルグループ (**link-local** キーワードが利用できない場合) が含まれています。

Examples

次に、**show ipv6 mld groups** コマンドの出力例を示します。この例では、ネットワークプロトコルで使用されているリンクローカルグループを含め、ファストイーサネットインターフェイス 2/1 が加入しているすべてのグループが示されています。

```

デバイス# show ipv6 mld groups FastEthernet 2/1
MLD Connected Group Membership
Group Address          Interface          Uptime           Expires
FF02::2                FastEthernet2/1   3d18h           never
FF02::D                 FastEthernet2/1   3d18h           never
FF02::16                FastEthernet2/1   3d18h           never

```

```

FF02::1:FF00:1      FastEthernet2/1      3d18h      00:00:27
FF02::1:FF00:79    FastEthernet2/1      3d18h      never
FF02::1:FF23:83C2  FastEthernet2/1      3d18h      00:00:22
FF02::1:FFAF:2C39  FastEthernet2/1      3d18h      never
FF06:7777::1       FastEthernet2/1      3d18h      00:00:26

```

次に、**show ipv6 mld groups** コマンドで **detail** キーワードを指定した場合の出力例を示します。

```

デバイス# show ipv6 mld groups detail
Interface:      Ethernet2/1/1
Group:          FF33::1:1:1
Uptime:         00:00:11
Router mode:    INCLUDE
Host mode:      INCLUDE
Last reporter:  FE80::250:54FF:FE60:3B14
Group source list:
Source Address      Uptime    Expires    Fwd  Flags
2004:4::6           00:00:11  00:04:08  Yes  Remote Ac 4

```

次に、**show ipv6 mld groups** コマンドで **explicit** キーワードを指定した場合の出力例を示します。

```

デバイス# show ipv6 mld groups explicit
Ethernet1/0, FF05::1
  Up:00:43:11 EXCLUDE(0/1) Exp:00:03:17
  Host Address      Uptime    Expires
  FE80::A8BB:CFFF:FE00:800  00:43:11  00:03:17
  Mode:EXCLUDE
Ethernet1/0, FF05::6
  Up:00:42:22 INCLUDE(1/0) Exp:not used
  Host Address      Uptime    Expires
  FE80::A8BB:CFFF:FE00:800  00:42:22  00:03:17
  Mode:INCLUDE
  300::1
  300::2
  300::3
Ethernet1/0 - Interface
ff05::1 - Group address
Up:Uptime for the group
EXCLUDE/INCLUDE - The mode the group is in on the router.
(0/1) (1/0) - (Number of hosts in INCLUDE mode/Number of hosts in EXCLUDE moe)
Exp:Expiry time for the group.
FE80::A8BB:CFFF:FE00:800 - Host ipv6 address.
00:43:11 - Uptime for the host.
00:03:17 - Expiry time for the host
Mode:INCLUDE/EXCLUDE - Mode the Host is operating in.
300::1, 300::2, 300::3 - Sources that the host has joined in the above specified mode.

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 45: show ipv6 mld groups フィールドの説明

フィールド	説明
Group Address	マルチキャストグループのアドレス。
Interface	グループに到達可能なインターフェイス。

show ipv6 mld groups

フィールド	説明
Uptime	このマルチキャストグループが認識されている時間（時間、分、および秒）。
Expires	エントリがMLDグループテーブルから削除されるまでの時間（時間、分、秒）。 ルータ自体がグループに参加している場合は満了タイマーに「never」が表示され、グループのルータモードがINCLUDEの場合は満了タイマーに「not used」と表示されます。この状況では、送信元のエントリの満了タイマーが使用されません。
Last reporter:	マルチキャストグループのメンバであることを最後に報告したホスト。
Flags Ac 4	設定したMLD状態の制限に向けてカウントされたフラグ。

Related Commands

Command	Description
ipv6 mld query-interval	Cisco IOS ソフトウェアがMLDホストクエリーメッセージを送信する頻度を設定します。

show ipv6 mld interface

インターフェイスに関するマルチキャスト関連情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mld interface** コマンドを使用します。

show ipv6 mld [*vrf vrf-name*] **interface** [*type number*]

Syntax Description	
vrf vrf-name	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
type number	(任意) インターフェイス タイプおよび番号

Command Modes	
	ユーザ EXEC (>)
	特権 EXEC (#)

Command History		
	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	
	オプションの <i>type</i> 引数と <i>number</i> 引数を省略すると、 show ipv6 mld interface コマンドはすべてのインターフェイスに関する情報を表示します。

Examples	
	次に、イーサネットインターフェイス 2/1/1 に対する show ipv6 mld interface コマンドの出力例を示します。

```

デバイス# show ipv6 mld interface Ethernet 2/1/1
Global State Limit : 2 active out of 2 max
Loopback0 is administratively down, line protocol is down
  Internet address is ::/0
.
.
.
Ethernet2/1/1 is up, line protocol is up
  Internet address is FE80::260:3EFF:FE86:5649/10
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Interface State Limit : 2 active out of 3 max
  State Limit permit access list:
  MLD activity: 83 joins, 63 leaves
  MLD querying router is FE80::260:3EFF:FE86:5649 (this system)

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 46: show ipv6 mld interface フィールドの説明

フィールド	説明
Global State Limit: 2 active out of 2 max	グローバルに設定されている 2 つの MLD 状態がアクティブです。
Ethernet2/1/1 is up, line protocol is up	インターフェイスのタイプ、番号、およびステータス。
Internet address is...	インターフェイスに適用されているインターフェイスとサブネットマスクのインターネットアドレス。
MLD is enabled in interface	マルチキャストリスナー検出 (MLD) が ipv6 multicast-routing コマンドによりインターフェイス上で有効になっていたかどうかを示します。
Current MLD version is 2	現在の MLD バージョン。
MLD query interval is 125 seconds	ipv6 mld query-interval コマンドで指定したように、Cisco IOS ソフトウェアが MLD クエリメッセージを送信する間隔 (秒単位)。
MLD querier timeout is 255 seconds	ipv6 mld query-timeout コマンドで指定したように、インターフェイスのクエリアとしてルータを継承するまでの時間 (秒単位)。
MLD max query response time is 10 seconds	ipv6 mld query-max-response-time コマンドで指定したように、ルータがグループを削除するまでに MLD クエリメッセージにホストが応答する必要がある時間 (秒単位)。
Last member query response interval is 1 seconds	グループおよび送信元固有のクエリを対象とする最大応答コードの計算に使用されます。また、リンクの「離脱遅延」の調整にも使用されます。小さい値は、グループを最後に離脱するメンバを検出する時間を短縮します。
Interface State Limit : 2 active out of 3 max	設定されているインターフェイスの状態の 3 つのうち 2 つがアクティブです。
State Limit permit access list: change	state permit アクセスリストのアクティビティ。
MLD activity: 83 joins, 63 leaves	受信しているグループの join と leave の数。
MLD querying router is FE80::260:3EFF:FE86:5649 (this system)	クエリ ルータの IPv6 アドレス。

Related Commands

Command	Description
ipv6 mld join-group	指定したグループおよび送信元に対して MLD レポートを設定します。

Command	Description
ipv6 mld query-interval	Cisco IOS ソフトウェアが MLD ホストクエリー メッセージを送信する頻度を設定します。

show ipv6 mld snooping

スイッチまたは VLAN の IP Version 6 (IPv6) マルチキャスト リスナー検出 (MLD) スヌーピング設定を表示するには、**show ipv6 mld snooping** コマンドを EXEC モードで使用します。

show ipv6 mld snooping [vlan *vlan-id*]

Syntax Description

vlan <i>vlan-id</i>	(任意) VLAN を指定します。指定できる範囲は 1 ~ 1001 および 1006 ~ 4094 です。
----------------------------	--

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スイッチまたは特定の VLAN の MLD スヌーピングの設定を表示するのにこのコマンドを使用します。

1002 ~ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

Examples

次に、**show ipv6 mld snooping vlan** コマンドの出力例を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```

デバイス# show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
Vlan 100:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3

```

```
Last listener query count : 2
Last listener query interval : 1000
```

次に、**show ipv6 mld snooping** コマンドの出力例を示します。ここでは、スイッチ上の VLAN すべてのスヌーピング特性を表示します。

```
デバイス# show ipv6 mld snooping
Global MLD Snooping configuration:
-----
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

Related Commands

Command	Description
ipv6 mld snooping	スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。
sdm prefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。

show ipv6 mld ssm-map

送信元特定マルチキャスト（SSM）マッピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mld ssm-map static** コマンドを使用します。

show ipv6 mld [**vrf vrf-name**] **ssm-map** [*source-address*]

Syntax Description	
vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
<i>source-address</i>	（任意）アクセスリストで識別されたグループの MLD メンバーシップに関連付けられている送信元アドレス。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines オプションの *source-address* 引数を使用しないと、すべての SSM マッピング情報が表示されます。

Examples

次に、ルータの SSM マッピングの例を示します。

```
デバイス# show ipv6 mld ssm-map
SSM Mapping : Enabled
DNS Lookup  : Enabled
```

次に、送信元アドレス 2001:0DB8::1 に対する SSM マッピングの例を示します。

```
デバイス# show ipv6 mld ssm-map 2001:0DB8::1
Group address : 2001:0DB8::1
Group mode ssm : TRUE
Database      : STATIC
Source list   : 2001:0DB8::2
               2001:0DB8::3

Router# show ipv6 mld ssm-map 2001:0DB8::2
Group address : 2001:0DB8::2
Group mode ssm : TRUE
Database      : DNS
Source list   : 2001:0DB8::3
               2001:0DB8::1
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 47: show ipv6 mld ssm-map フィールドの説明

フィールド	説明
SSM Mapping	SSM マッピング機能が有効になります。
DNS Lookup	SSM マッピング機能が有効になっている場合、DNS ルックアップ機能は自動的に有効になります。
Group address	特定のアクセス リストで識別されているグループアドレス。
Group mode ssm : TRUE	特定のグループがSSM モードで機能しています。
Database : STATIC	静的 SSM マッピング設定を確認することで送信元アドレスを特定するようにルータが設定されます。
Database : DNS	DNS ベースの SSM マッピングを使用して送信元アドレスを特定するようにルータが設定されます。
Source list	アクセスリストによって識別されているグループに関連付けられている送信元アドレス。

Related Commands

コマンド	説明
debug ipv6 mld ssm-map	SSM マッピングのデバッグ メッセージを表示します。
ipv6 mld ssm-map enable	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ipv6 mld ssm-map query dns	DNS ベースの SSM マッピングを有効にします。
ipv6 mld ssm-map static	スタティック SSM マッピングを設定します。

show ipv6 mld traffic

マルチキャストリスナー検出（MLD）トラフィックカウンタを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mld traffic** コマンドを使用します。

show ipv6 mld [vrf vrf-name] traffic

Syntax Description

vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
----------------------------	---

Command Modes

ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

予測した数の MLD プロトコルメッセージを送受信したかどうかを確認するには、**show ipv6 mld traffic** コマンドを使用します。

Examples

次に、送受信された MLD プロトコルメッセージを表示する例を示します。

```
デバイス# show ipv6 mld traffic
```

```
MLD Traffic Counters
Elapsed time since counters cleared:00:00:21
                Received      Sent
Valid MLD Packets      3          1
Queries                 1          0
Reports                 2          1
Leaves                  0          0
Mtrace packets         0          0
Errors:
Malformed Packets                0
Bad Checksums                    0
Martian source                    0
Packets Received on MLD-disabled Interface 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 48: show ipv6 mld traffic フィールドの説明

フィールド	説明
Elapsed time since counters cleared	カウンタをクリアしてからの時間を示します（時間、分、秒単位）。
Valid MLD packets	送受信された有効な MLD パケットの数。

フィールド	説明
Queries	送受信された有効なクエリの数。
Reports	送受信された有効なレポートの数。
Leaves	送受信された有効な leave の数。
Mtrace packets	送受信されたマルチキャスト トレース パケットの数。
Errors	発生したエラーのタイプと数。

show ipv6 mrib client

マルチキャストルーティング情報ベース（MRIB）のクライアントに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mrib client** コマンドを使用します。

show ipv6 mrib [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* : *client-id*}]

Syntax Description

vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
filter	（任意）各クライアントが所有し、各クライアントが対象としている MRIB フラグに関する情報を表示します。
name	（任意）マルチキャストリスナー検出（MLD）や Protocol Independent Multicast（PIM）などのように MRIB のクライアントとして機能するマルチキャストルーティングプロトコルの名前。
<i>client-name</i> : <i>client-id</i>	（任意）MLD または PIM など、MRIB のクライアントとして動作するマルチキャストルーティングプロトコルの名前と ID。コロン記号が必要です。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

各クライアントが所有する MRIB フラグと、各クライアントが対象とするフラグに関する情報を表示するには、**filter** キーワードを使用します。

Examples

次に、**show ipv6 mrib client** コマンドの出力例を示します。

```

デバイス# show ipv6 mrib client
IP MRIB client-connections
igmp:145          (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3      (connection id 2)
slot 3  mfib ipv6 rp agent:16  (connection id 3)
slot 1  mfib ipv6 rp agent:16  (connection id 4)
slot 0  mfib ipv6 rp agent:16  (connection id 5)
slot 4  mfib ipv6 rp agent:16  (connection id 6)
slot 2  mfib ipv6 rp agent:16  (connection id 7)

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 49: show ipv6 mrib client フィールドの説明

フィールド	説明
igmp:145 (connection id 0) pim:146 (connection id 1) mrib ipv6:3 (connection id 2) mrib ipv6 rp agent:16 (connection id 3)	クライアント ID (クライアント名: プロセス ID)

show ipv6 mrib route

マルチキャストルーティング情報ベース（MRIB）のルート情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mrib route** コマンドを使用します。

show ipv6 mrib [**vrf** *vrf-name*] **route** [**link-local** | **summary**] [*source-address* | *source-name* | *] [*groupname-or-address* [*prefix-length*]]

Syntax Description

vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
link-local	（任意）リンク ローカル グループを表示します。
summary	（任意）MRIB エントリ（リンクローカルグループを含む）と MRIB テーブルに存在するインターフェイスの数を表示します。
<i>source address-or-name</i>	（任意）送信元の IPv6 アドレスまたは名前。
*	（任意）MRIB ルート情報を表示します。
<i>groupname or-address</i>	（任意）マルチキャストグループの IPv6 アドレスまたは名前。
<i>prefix-length</i>	（任意）IPv6 プレフィックス長。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

マルチキャストリスナー検出（MLD）、Protocol Independent Multicast（PIM）、マルチキャスト転送情報ベース（MFIB）など、すべてのエントリが MRIB のさまざまなクライアントによって作成されます。各エントリまたはインターフェイスのフラグは MRIB のさまざまなクライアント間の通信メカニズムとして機能します。エントリには、新しい送信元や実行したアクションについて PIM が登録メッセージをどのように送信したかが示されます。

summary キーワードは、リンクローカルエントリを含めて、すべてのエントリのカウントを表示します。

次の表で、インターフェイスフラグについて説明します。

Table 50: インターフェイス フラグの説明

フラグ	説明
F	Forward: データはこのインターフェイスから転送されます。
A	Accept: このインターフェイス上で受信されたデータは、転送用として受け入れられます。
IC	Internal copy (内部コピー)
NS	Negate signal (信号を無効化)
DP	Do not preserve (保存せず)
SP	Signal present (信号あり)
II	Internal interest (内部対象)
ID	Internal uninterest (内部対象外)
LI	Local interest (ローカル対象)
LD	Local uninterest (ローカル非対称)
C	直接接続チェックを実行します。

MRIB 内の特殊なエントリは、通常動作からの例外を示します。たとえば、no signaling または no notification は、特殊なグループの範囲のいずれかと一致するデータ パケットの着信に必要です。特殊なグループの範囲は次のとおりです。

- 未定義の範囲 (FFX0::/16)
- ノード ローカル グループ (FFX1::/16)
- リンクローカル グループ (FFX2::/16)
- Source Specific Multicast (SSM) グループ (FF3X::/32)

残りの (通常はスパースモードの) すべての IPv6 マルチキャストグループについては、直接接続チェックが実行され、直接接続の送信元が着信した場合は PIM に通知されます。このプロセスは、新しい送信元の登録メッセージを PIM がどのように送信するかを指定します。

Examples

次に、**show ipv6 mrib route** コマンドで **summary** キーワードを指定した場合の出力例を示します。

```

デバイス# show ipv6 mrib route summary
MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 51: show ipv6 mrib route フィールドの説明

フィールド	説明
No. of (*, G) routes	MRIB 内の共有ツリー ルートの数。
No. of (S, G) routes	MRIB 内の送信元ツリー ルートの数。
No. of Route x Interfaces (Rxl)	各 MRIB ルート エントリ上のすべてのインターフェイスの合計。

show ipv6 mroute

show ip mroute コマンドに似た形式で PIM トポロジテーブルに情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mroute** コマンドを使用します。

show ipv6 mroute [**vrf** *vrf-name*] [**link-local** | [*group-name* | *group-address* [*source-address* | *source-name*]]] [**summary**] [**count**]

Syntax Description	
vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
link-local	(任意) リンク ローカル グループを表示します。
<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。
<i>source-address</i> <i>source-name</i>	(任意) 送信元の IPv6 アドレスまたは名前。
summary	(任意) IPv6 マルチキャストルーティング テーブル内の各エントリの要約を 1 行で表示します。
count	(任意) パケット数、パケット/秒、平均パケットサイズ、および、バイト/秒などのグループと送信元に関するマルチキャスト転送情報ベース (MFIB) からの統計を表示します。

Command Default **show ipv6 mroute** コマンドはすべてのグループおよび送信元を表示します。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines IPv6 マルチキャストの実装には、個別の mroute テーブルがありません。そのため、**show ipv6 mroute** コマンドで、**show ip mroute** コマンドに似た形式の PIM トポロジテーブルに情報を表示できます。

オプションの引数とキーワードをすべて省略すると、**show ipv6 mroute** コマンドは PIM トポロジテーブル内のすべてのエントリを表示します (**link-local** キーワードが利用できるリンクローカルグループを除く)。

Cisco IOS ソフトウェアは、PIM プロトコルメッセージ、MLD レポート、およびトラフィックに基づいて (S,G) および (*,G) エントリを作成して PIM トポロジテーブルにデータを入力します。アスタリスク (*) は、すべてのソースアドレスを示し、「S」は単一ソースアドレスを示し、「G」は宛先マルチキャストグループアドレスを示します。(S, G) エントリの作成時に、ソフト

ウェアはユニキャストルーティングテーブルで見つかった（つまり、Reverse Path Forwarding（RPF）によって）、該当する宛先グループへの最適なパスを使用します。

各 IPv6 マルチキャストルートの転送ステータスを表示するには、**show ipv6 mroute** コマンドを使用します。

Examples

次に、**show ipv6 mroute** コマンドの出力例を示します。

```

デバイス# show ipv6 mroute ff07::1
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
      C - Connected, L - Local, I - Received Source Specific Host Report,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27

```

次に、**summary** キーワードを指定した場合の **show ipv6 mroute** コマンドの出力例を示します。

```

デバイス# show ipv6 mroute ff07::1 summary
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
      C - Connected, L - Local, I - Received Source Specific Host Report,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:55/00:02:36, RP 2001:0DB8:6::6, OIF count:1, flags:S
(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, OIF count:1, flags:SFT

```

次に、**count** キーワードを指定した場合の **show ipv6 mroute** コマンドの出力例を示します。

```

デバイス# show ipv6 mroute ff07::1 count
IP Multicast Statistics
71 routes, 24 groups, 0.04 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF=null, rate-limit etc)
Group:FF07::1
RP-tree:
  RP Forwarding:0/0/0/0, Other:0/0/0
  LC Forwarding:0/0/0/0, Other:0/0/0
Source:2001:0DB8:999::99,
  RP Forwarding:0/0/0/0, Other:0/0/0
  LC Forwarding:0/0/0/0, Other:0/0/0
HW Forwd: 20000/0/92/0, Other:0/0/0
Tot. shown:Source count:1, pkt count:20000

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 52: show ipv6 mroute フィールドの説明

フィールド	説明
Flags:	<p>エントリーに関する情報を提供します。</p> <ul style="list-style-type: none"> • S: スパース。エントリーはスパース モードで動作しています。 • s: SSM グループ。マルチキャスト グループが SSM の IP アドレス範囲内であることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。 • C: 接続中。マルチキャストグループのメンバは、直接接続されたインターフェイス上に存在します。 • L: ローカル。ルータ自体が、マルチキャストグループのメンバです。 • I: 送信元固有のホスト レポートを受信。(S,G) エントリーが (S,G) レポートによって作成されたことを示します。このフラグは、代表ルータ (DR) 上にものみ設定できます。 • P: プルーニング済み。ルートがプルーニングされています。Cisco IOS ソフトウェアは、この情報を保持して、ダウンストリームメンバが送信元に加入できるようにします。 • R: RP ビットを設定。(S,G) エントリーが RP をポイントしていることを示します。通常、これは特定の送信元に関する共有ツリーに沿ったプルーニングステートを示します。 • F: 登録フラグ。ソフトウェアがマルチキャスト送信元に登録されていることを示します。 • T: SPT ビットを設定。パケットが最短パス送信元ツリーで受信されていることを示します。 • J: SPT に参加。(*,G) エントリーの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します (デフォルトの SPT しきい値設定は 0 kbps です)。J の最短パスツリー (SPT) 参加フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join がトリガーされます。これにより、ルータは送信元ツリーに参加します。デフォルトの SPT しきい値の 0 kbps がグループに使用され、J - SPT 参加フラグは常に (*, G) エントリー上に設定され、クリアされることはありません。ルータは、新しい送信元からのトラフィックを受信すると、最短パス送信元ツリーに切り替えます。

フィールド	説明
Timers: Uptime/Expires	「Uptime」はインターフェイスごとの、IPv6 マルチキャストルーティングテーブル内にエントリが存在する時間（時間、分、秒）を示します。 「Expires」は、IPv6 マルチキャストルーティングテーブルからエントリが削除されるまでの時間（時間、分、秒）をインターフェイスごとに示します。
Interface state:	着信インターフェイスまたは発信インターフェイスの状態を示します。 <ul style="list-style-type: none"> • [Interface]。タイプと、着信インターフェイスまたは発信インターフェイスのリストに記載されているインターフェイスの数を示します。 • Next-Hop。「Next-Hop」は、ダウンストリームネイバーのIPアドレスを指定します。 • State/Mode。「State」はアクセスリストによる制限があるかどうかに応じて、インターフェイス上で転送、ブルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。「Mode」は、インターフェイスがスパースモードで動作していることを示します。
(*, FF07::1) and (2001:0DB8:999::99)	IPv6 マルチキャストルーティングテーブルのエントリ。エントリは、送信元ルータのIPv6アドレスと、それに続くマルチキャストグループのIPv6アドレスで構成されます。送信元ルータの位置に置かれたアスタリスク(*)は、すべての送信元を意味します。 最初の形式のエントリは、(*, G)または「スターカンマG」エントリと呼ばれます。2番目の形式のエントリは(S, G)または「SカンマG」エントリと呼ばれ、(S, G)エントリの構築に使用されます。
RP	RP ルータのアドレス。
flags:	このMRIB エントリ上のMRIB クライアントが設定した情報。
Incoming interface:	送信元からのマルチキャストパケット用のインターフェイスです。パケットがこのインターフェイスに着信しなかった場合、破棄されます。
RPF nbr	RP または送信元に対するアップストリームルータのIPアドレス。
Outgoing interface list:	パケットが転送される際に通過したインターフェイス。(S,G)のエントリについては、このリストは(*,G)エントリから継承したインターフェイスは含めません。

Related Commands

コマンド	説明
ipv6 multicast-routing	ルータのすべてのIPv6対応インターフェイス上でPIMとMLDを使用したマルチキャストルーティングを有効にし、マルチキャスト転送を有効にします。

コマンド	説明
show ipv6 mfib	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。

show ipv6 mtu

IPv6 インターフェイスの最大伝送ユニット（MTU）のキャッシュ情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mtu** コマンドを使用します。

show ipv6 mtu [*vrf vrfname*]

Syntax Description

vrf	（任意）IPv6 バーチャルプライベート ネットワーク（VPN）ルーティング/転送インスタンス（VRF）。
vrfname	（任意）IPv6 VRF の名前。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

vrf キーワードと *vrfname* 引数を使用すると、特定の VRF に関連する MTU を表示できます。

Examples

次に、**show ipv6 mtu** コマンドの出力例を示します。

```
デバイス# show ipv6 mtu
MTU      Since      Destination Address
1400     00:04:21  5000:1::3
1280     00:04:50  FE80::203:A0FF:FED6:141D
```

次に、**vrf** キーワードと *vrfname* 引数を使用した **show ipv6 mtu** コマンドの出力例を示します。次の例では、*vrfname1* という VRF に関する情報が表示されます。

```
デバイス# show ipv6 mtu vrf vrfname1
MTU      Since      Source Address      Destination Address
1300     00:00:04   2001:0DB8:2        2001:0DB8:7
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 53: show ipv6 mtu フィールドの説明

フィールド	説明
MTU	宛先アドレスへのパスに使用され、Internet Control Message Protocol（ICMP）の packet-too-big メッセージに含まれている MTU。
Since	ICMP packet-too-big メッセージを受信してからのエントリの期間経過。

フィールド	説明
Destination Address	受信した ICMP packet-too-big メッセージに含まれているアドレス。このルータからこのアドレスに発信されるパケットは指定した MTU 未満の大きさである必要があります。

Related Commands

コマンド	説明
ipv6 mtu	インターフェイス上で送信する IPv6 パケットの MTU サイズを設定します。

show ipv6 nd destination

IPv6 ホストモードの宛先キャッシュのエントリに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 nd destination** コマンドを使用します。

show ipv6 nd destination[vrf vrf-name][interface-type interface-number]

Syntax Description

vrf vrf-name	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
interface-type	(任意) インターフェイス タイプを指定します。
interface-number	(任意) インターフェイス番号を指定します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IPv6 ホストモードの宛先キャッシュのエントリに関する情報を表示するには、**show ipv6 nd destination** コマンドを使用します。**vrf vrf-name** キーワードと引数のペアを使用すると、指定した VRF に関する情報のみが表示されます。**interface-type** 引数と **interface-number** 引数を使用すると、指定したインターフェイスに関する情報のみが表示されます。

Examples

```
デバイス# show ipv6 nd destination
```

```
IPv6 ND destination cache (table: default)
Code: R - Redirect
  2001::1 [8]
    via FE80::A8BB:CCFF:FE00:5B00/Ethernet0/0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

Table 54: show ipv6 nd destination フィールドの説明

フィールド	説明
Code: R - Redirect	リダイレクトを通じて学習した宛先。
2001::1 [8]	カッコ内に表示される値は、宛先キャッシュエントリが最後に使用されてからの秒単位の時間です。

Related Commands

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホストモードを有効にします。

show ipv6 nd on-link prefix

ルータアドバタイズメント（RA）を通じて学習したオンリンクプレフィックスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 nd on-link prefix** コマンドを使用します。

show ipv6 nd on-link prefix[vrf *vrf-name*][*interface-type interface-number*]

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>interface -type</i>	(任意) インターフェイス タイプを指定します。
<i>interface -number</i>	(任意) インターフェイス番号を指定します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

RA を通じて学習したオンリンクプレフィックスに関する情報を表示するには、**show ipv6 nd on-link prefix** コマンドを使用します。

RA から学習したプレフィックスは **show ipv6 nd on-link prefix** コマンドを使用して検査できます。**vrf vrf-name** キーワードと引数のペアを使用すると、指定した VRF に関する情報のみが表示されます。*interface-type* 引数と *interface-number* 引数を使用すると、指定したインターフェイスに関する情報のみが表示されます。

Examples

次に、RA を通じて学習したオンリンクプレフィックスに関する情報を表示する例を示します。

```
デバイス# show ipv6 nd on-link prefix

IPv6 ND on-link Prefix (table: default), 2 prefixes
Code: A - Autonomous Address Config
A 2001::/64 [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
2001:1:2::/64 [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
```

Related Commands

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホストモードを有効にします。

show ipv6 neighbors

IPv6 ネイバー探索 (ND) のキャッシュ情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 neighbors** コマンドを使用します。

show ipv6 neighbors [*interface-type interface-number* *ipv6-address* *ipv6-hostname* | **statistics**]

Syntax Description	
<i>interface-type</i>	(任意) IPv6 ネイバー情報が表示されるインターフェイスのタイプを指定します。
<i>interface-number</i>	(任意) IPv6 ネイバー情報が表示されるインターフェイスの番号を指定します。
<i>ipv6-address</i>	(任意) ネイバーの IPv6 アドレスを指定します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>ipv6-hostname</i>	(任意) リモート ネットワーク デバイスの IPv6 ホスト名を指定します。
statistics	(任意) ND キャッシュの統計を表示します。

Command Default すべての IPv6 ND キャッシュのエントリがリストされます。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines *interface-type* と *interface-number* 引数が指定されていない場合は、すべての IPv6 ネイバーのキャッシュ情報が表示されます。*interface-type* と *interface-number* 引数を指定すると、特定のインターフェイスのキャッシュ情報だけが表示されます。

statistics キーワードを指定すると、ND キャッシュの統計が表示されます。

次に、インターフェイスタイプおよび番号を指定して入力した **show ipv6 neighbors** コマンドの出力例を示します。

```

デバイス# show ipv6 neighbors ethernet 2
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e REACH Ethernet2
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e REACH Ethernet2
3001:1::45a                                  - 0002.7d1a.9472 REACH Ethernet2

```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbors** コマンドの出力例を示します。

```

デバイス# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address          Age Link-layer Addr State Interface
2000:0:0:4::2        0 0003.a0d6.141e REACH Ethernet2

```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 55: show ipv6 neighbors フィールドの説明

フィールド	説明
IPv6 Address	隣接またはインターフェイスの IPv6 アドレス。
Age	アドレスが到達可能と確認されてから経過した時間（分）。ハイフン (-) はスタティック エントリを示します。
Link-layer Addr	MAC アドレス。アドレスが不明の場合、ハイフン (-) が表示されます。

フィールド	説明
State	<p>隣接キャッシュエントリの状態。次に、IPv6 ネイバー探索キャッシュのダイナミック エントリの状態を示します。</p> <ul style="list-style-type: none"> • INCMP (Incomplete): アドレス解決がエントリで実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノードマルチキャストアドレスに送信されましたが、対応するネイバーアドバタイズメントメッセージが受信されていません。 • REACH (Reachable): ネイバーへの転送パスが正しく機能していたことを示す確認が、最後の ReachableTime ミリ秒内に受信されました。REACH 状態になっている間は、パケットが送信されるたびにデバイスは特別なアクションを実行しません。 • STALE: 転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が ReachableTime ミリ秒を超えています。STALE 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。 • DELAY: 転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が ReachableTime ミリ秒を超えています。パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。DELAY 状態に入ってから、DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が PROBE に変更されます。 • PROBE: 到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとに、ネイバー送信要求メッセージを再送信することで、到達可能性確認がアクティブに求められます。 • ????: 不明な状態。 <p>次に、IPv6 ネイバー探索キャッシュのスタティック エントリの可能な状態を示します。</p> <ul style="list-style-type: none"> • INCMP (不完全): このエントリのインターフェイスがダウンしています。 • REACH (到達可能): このエントリのインターフェイスがアップしています。 <p>Note 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、INCMP (不完全) 状態と REACH (到達可能) 状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。</p>
Interface	アドレスに到達可能であったインターフェイス。

次に、**statistics** キーワードを指定した場合の **show ipv6 neighbors** コマンドの出力例を示します。

デバイス# **show ipv6 neighbor statistics**

```
IPv6 ND Statistics
Entries 2, High-water 2, Gleaned 1, Scavenged 0
Entry States
  INCMP 0 REACH 0 STALE 2 GLEAN 0 DELAY 0 PROBE 0
Resolutions (INCMP)
  Requested 1, timeouts 0, resolved 1, failed 0
  In-progress 0, High-water 1, Throttled 0, Data discards 0
Resolutions (PROBE)
  Requested 3, timeouts 0, resolved 3, failed 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 56: show ipv6 neighbors statistics フィールドの説明

フィールド	説明
Entries	ND キャッシュ内の ND ネイバー エントリの総数。
High-Water	ND キャッシュ内の ND ネイバー エントリの（現在までの）最大量。
Gleaned	収集した（つまり、ネイバー NA はたは他の ND パケットから学習した）ND ネイバー エントリの数。
Scavenged	タイムアウトし、キャッシュから削除されている古い ND ネイバー エントリの数。
Entry States	各状態の ND ネイバー エントリの数。
Resolutions (INCMP)	<p>INCMP 状態で試行されたネイバー解決（データパケットによるプロンプトでの解決）の統計。INCMP 状態で試行された解決の詳細は次のとおりです。</p> <ul style="list-style-type: none"> • Requested: 要求された解決の総数。 • Timeouts: 解決時のタイムアウトの数。 • Resolved: 正常に解決された数。 • Failed: 失敗した解決の数。 • In-progress: 進行中の解決の数。 • High-water: 進行中の解決の（現在までの）最大数。 • Throttled: 進行中の解決の最大数制限のため、解決要求が無視された回数。 • Data discards: ネイバー解決待機中のデータパケットが破棄された数。

フィールド	説明
Resolutions (PROBE)	<p>PROBE 状態で試行されたネイバー解決（データパケットによるプロンプトでの既存エントリの再解決）の統計。</p> <ul style="list-style-type: none">• Requested: 要求された解決の総数。• Timeouts: 解決時のタイムアウトの数。• Resolved: 正常に解決された数。• Failed: 失敗した解決の数。

show ipv6 ospf

Open Shortest Path First (OSPF) ルーティングプロセスに関する一般情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ipv6 ospf** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] [*rate-limit*]

Syntax Description

<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティングプロセスが有効になっているときに管理する目的で割り当てられた番号です。
<i>area-id</i>	(任意) エリア ID。(任意) この引数は指定したエリアに関する情報のみを表示します。
<i>rate-limit</i>	(任意) レート制限リンクステートアドバタイズメント (LSA)。このキーワードは、現在レートが制限されている LSA とともに、次の生成までの残り時間を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

show ipv6 ospf の出力例

次に、**show ipv6 ospf** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msec
  Retransmission pacing timer 66 msec
  Number of external LSA 0. Checksum Sum 0x000000
  Number of areas in this device is 1. 1 normal 0 stub 0 nssa
    Area BACKBONE(0)
      Number of interfaces in this area is 1
      MD5 Authentication, SPI 1000
      SPF algorithm executed 2 times
      Number of LSA 5. Checksum Sum 0x02A005
      Number of DChitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 57: show ipv6 ospf フィールドの説明

フィールド	説明
Routing process "ospfv3 1" with ID 10.10.10.1	プロセス ID と OSPF デバイス ID。
LSA group pacing timer	設定されている LSA グループ ペーシング タイマー（秒単位）。
Interface flood pacing timer	設定されている LSA フラッド ペーシング タイマー（ミリ秒単位）。
Retransmission pacing timer	設定されている LSA 再送信ペーシング タイマー（ミリ秒単位）。
Number of areas	デバイス内のエリアの数、エリアアドレスなど。

エリア 暗号化を使用した show ipv6 ospf の例

次に、エリア暗号化情報を使用した **show ipv6 ospf** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border device
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this device is 2. 2 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    SPF algorithm executed 3 times
    Number of LSA 31. Checksum Sum 0x107493
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 20
    Flood list length 0
  Area 1
    Number of interfaces in this area is 2
    NULL Encryption SHA-1 Auth, SPI 1001
    SPF algorithm executed 7 times
    Number of LSA 20. Checksum Sum 0x095E6A
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 58: エリア 暗号化情報を使用した *show ipv6 ospf* フィールドの説明

フィールド	説明
Area 1	後続のフィールドでエリア 1 を説明します。
NULL Encryption SHA-1 Auth, SPI 1001	暗号化アルゴリズム（この場合はヌル。つまり暗号化アルゴリズムは使用されていない）、認証アルゴリズム（SHA-1）、およびセキュリティポリシーインデックス（SPI）値（1001）を表示します。

次に、SPF および LSA のスロットリング タイマーの設定値を表示する例を示します。

```

デバイス# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary device
Redistributing External Routes from,
  ospf 2
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF 10000 msec
Maximum wait time between two consecutive SPF 10000 msec
Minimum LSA interval 5 sec
Minimum LSA arrival 1000 msec

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 59: SPF および LSA スロットリングを使用した *show ipv6 ospf* フィールドの説明

フィールド	説明
Initial SPF schedule delay	SPF 計算の遅延時間。
Minimum hold time between two consecutive SPF	連続する SPF 計算間の最小保持時間。
Maximum wait time between two consecutive SPF 10000 msec	連続する SPF 計算間の最大保持時間。
Minimum LSA interval 5 sec	リンクステート アドバタイズメント間の最小時間間隔（秒単位）。
Minimum LSA arrival 1000 msec	リンクステート アドバタイズメントの最大着信時間（ミリ秒単位）。

次に、現在レートが制限されている LSA に関する情報の例を示します。

```

デバイス# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
  LSAs: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
  LSAs: 0.0.0.0 Type: 0x2009 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 60: show ipv6 ospf rate-limit フィールドの説明

フィールド	説明
LSAID	LSA のリンクステート ID。
Type	LSA の説明。
Adv Rtr	アドバタイジング デバイスの ID。
Due in:	次のイベント生成までの残り時間。

show ipv6 ospf border-routers

エリア境界ルータ（ABR）および自律システム境界ルータ（ASBR）に対する内部 Open Shortest Path First（OSPF）ルーティングテーブルエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf border-routers** コマンドを使用します。

show ip ospf [*process-id*] **border-routers**

Syntax Description

<i>process-id</i>	（任意）内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPFルーティングプロセスが有効になっているときに管理する目的で割り当てられた番号です。
-------------------	--

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**show ipv6 ospf border-routers** コマンドの出力例を示します。

```
デバイス# show ipv6 ospf border-routers
```

```
OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 61: show ipv6 ospf border-routers フィールドの説明

フィールド	説明
i - Intra-area route, I - Inter-area route	このルートのタイプ。
172.16.4.4, 172.16.3.3	宛先ルータのルータ ID。
[2], [1]	宛先ルータに到達するために使用するメトリック。
FE80::205:5FFF:FED3:5808, FE80::205:5FFF:FED3:5406, FE80::205:5FFF:FED3:5808	リンクローカルルータ。
FastEthernet0/0, POS4/0	IPv6 OSPF プロトコルを設定するインターフェイス。

フィールド	説明
ABR	エリア境界ルータ。
ASBR	自律システム境界ルータ。
Area 0, Area 1	このルートが学習されるエリアのエリア ID。
SPF 13, SPF 8, SPF 3	このルートをインストールする Shortest Path First (SPF) 計算の内部番号。

show ipv6 ospf event

IPv6 Open Shortest Path First (OSPF) イベントに関する詳細情報を表示するには、特権 EXEC モードで **show ipv6 ospf event** コマンドを使用します。

show ipv6 ospf [*process-id*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]

Syntax Description

<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティングプロセスが有効になっているときに管理する目的で割り当てられた番号です。
generic	(任意) IPv6 イベントに関する一般的な情報。
interface	(任意) 新旧の状態を含むインターフェイス状態変更イベント。
lsa	(任意) LSA 着信イベントおよび LSA 生成イベント。
neighbor	(任意) 新旧の状態を含むネイバー状態変更イベント。
reverse	(任意) イベントの表示を最新のものから最も古いものへ、または最も古いものから最新のものへと逆転させるためのキーワード。
rib	(任意) ルーティング情報ベース (RIB) の更新イベント、削除イベント、および再配布イベント。
spf	(任意) スケジューリングおよび SPF 実行イベント。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

OSPF イベントログは OSPF インスタンスごとに保持されます。キーワードを指定せずに **show ipv6 ospf event** コマンドを入力すると、OSPF イベントログ内のすべての情報が表示されます。特定の情報をフィルタ処理するには、このキーワードを使用します。

Examples

次の例は、スケジューリングと SPF 実行イベント、LSA 着信イベント、および LSA 生成イベントを最も古いイベントから最新の生成済みイベントの順に示しています。

```
デバイス# show ipv6 ospf event spf lsa reverse
```

```
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
1 *Sep 29 11:59:18.367: Rcv Changed Type=0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
3 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
```

```

4 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 2
5 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
6 *Sep 29 11:59:18.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
8 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
9 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
80007699, Age 2
10 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
11 *Sep 29 11:59:18.867: Starting SPF
12 *Sep 29 11:59:18.867: Starting Intra-Area SPF in Area 0
16 *Sep 29 11:59:18.867: Starting Inter-Area SPF in area 0
17 *Sep 29 11:59:18.867: Starting External processing
18 *Sep 29 11:59:18.867: Starting External processing in area 0
19 *Sep 29 11:59:18.867: Starting External processing in area 1
20 *Sep 29 11:59:18.867: End of SPF
21 *Sep 29 11:59:19.367: Generate Changed Type-0x2003 LSA, LSID 10.0.0.4, Seq# 80000002,
Age 3600, Area 1, Prefix 3000:11:22::/64
23 *Sep 29 11:59:20.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699A, Age 2
24 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
25 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699A, Age 2
26 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
27 *Sep 29 11:59:20.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 80007699A, Age 2
28 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
29 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
80007699A, Age 2
30 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
31 *Sep 29 11:59:20.867: Starting SPF
32 *Sep 29 11:59:20.867: Starting Intra-Area SPF in Area 0
36 *Sep 29 11:59:20.867: Starting Inter-Area SPF in area 0
37 *Sep 29 11:59:20.867: Starting External processing
38 *Sep 29 11:59:20.867: Starting External processing in area 0
39 *Sep 29 11:59:20.867: Starting External processing in area 1
40 *Sep 29 11:59:20.867: End of SPF

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 62: show ip ospf フィールドの説明

フィールド	説明
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)	プロセス ID および OSPF ルータ ID。
Rcv Changed Type-0x2009 LSA	新たに着信した LSA の説明。
LSID	LSA のリンクステート ID。
Adv-Rtr	アドバタイジング ルータの ID です。
Seq#	リンク ステートシーケンス番号（以前の、または重複した LSA を検出します）
Age	リンク状態の期間経過（秒単位）。
Schedule SPF	実行する SPF を有効にします。

show ipv6 ospf event

フィールド	説明
Area	OSPF エリア ID。
Change in LSID	LSA の変更後のリンクステート ID。
LSA type	LSA タイプ。

show ipv6 ospf graceful-restart

Open Shortest Path First for IPv6（OSPFv3）グレースフルリスタート情報を表示するには、特権 EXEC モードで **show ipv6 ospf graceful-restart** コマンドを使用します。

show ipv6 ospf graceful-restart

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC（#）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines OSPFv3 グレースフルリスタート機能に関する情報を検出するには、**show ipv6 ospf graceful-restart** コマンドを使用します。

Examples

次に、OSPFv3 グレースフルリスタート情報を表示する例を示します。

```

デバイス# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
Graceful Restart enabled
  restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
Graceful Restart helper support enabled
Router status : Active
Router is running in SSO mode
OSPF restart state : NO_RESTART
Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
  
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 63: show ipv6 ospf graceful-restart フィールドの説明

フィールド	説明
Routing Process "ospf 1"	OSPFv3 ルーティング プロセス ID。
Graceful Restart enabled	このルータでグレースフルリスタート機能が有効になっています。
restart-interval limit: 120 sec	リスタート間隔の制限。
last restart 00:00:15 ago (took 36 secs)	最後にグレースフルリスタートが実行されてからの経過時間と、実行に要した時間。

show ipv6 ospf graceful-restart

フィールド	説明
Graceful Restart helper support enabled	グレースフルリスタートヘルパーモードが有効になっています。このルータ上でもグレースフルリスタートモードが有効になっているため、このルータはグレースフルリスタート対応として識別できます。グレースフルリスタート認識型のルータはグレースフルリスタートモードでは設定できません。
Router status : Active	このルータは、スタンバイとは対照的に、アクティブモードです。
Router is running in SSO mode	ルータはステートフルスイッチオーバーモードです。
OSPF restart state : NO_RESTART	現在の OSPFv3 のリスタート状態。
Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0	現在のルータとチェックポイントルータの IPv6 アドレス。

Related Commands

コマンド	説明
show ipv6 ospf interface	OSPFv3 関連のインターフェイス情報を表示します。

show ipv6 ospf interface

Open Shortest Path First (OSPF) 関連のインターフェイス情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ipv6 ospf interface** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]

Syntax Description	
<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティングプロセスが有効になっているときに管理する目的で割り当てられた番号です。
<i>area-id</i>	(オプション) 指定したエリアに関する情報だけを表示します。
<i>type number</i>	(任意) インターフェイス タイプおよび番号
brief	(任意) OSPF インターフェイス、状態、アドレスとマスク、およびルータのエリアに関する簡単な概要情報を表示します。

Command Modes	
	ユーザ EXEC (>)
	特権 EXEC (#)

Command History	
	リリース
	変更内容
	Cisco IOS XE Fuji 16.9.2
	このコマンドが導入されました。

Examples

show ipv6 ospf interface 標準出力例

次に、**show ipv6 ospf interface** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1

```

show ipv6 ospf interface

```

Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:05
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 12, maximum is 12
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.6.6 (Designated Router)
Suppress hello for 0 neighbor(s)

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 64: show ipv6 ospf interface フィールドの説明

フィールド	説明
ATM3/0	物理リンクのステータス、およびプロトコルの動作ステータス。
Link Local Address	インターフェイス IPv6 アドレス。
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	このルータを学習するエリアのエリア ID、プロセス ID、インスタンス ID、およびルータ ID。
Network Type POINT_TO_POINT, Cost: 1	ネットワーク タイプとリンクステート コスト。
Transmit Delay	転送遅延、インターフェイス ステート、およびルータ プライオリティ。
Designated Router	指定ルータ ID および各インターフェイス IP アドレス。
Backup Designated router	バックアップ指定ルータ ID および各インターフェイス IP アドレス。
Timer intervals configured	タイマーインターバルの設定。
Hello	次の hello パケットがこのインターフェイスから送信されるまでの時間（秒単位）。
Neighbor Count	ネットワーク ネイバーの数、および隣接ネイバーのリスト。

Cisco IOS Release 12.2(33) SRB の例

次に、**brief** キーワードを入力した場合の **show ipv6 ospf interface** コマンドの出力例を示します。

```
デバイス# show ipv6 ospf interface brief
```

```

Interface  PID  Area          Intf ID  Cost  State  Nbrs  F/C
VL0        6    0             21      65535 DOWN   0/0

```

Se3/0	6	0	14	64	P2P	0/0
Lo1	6	0	20	1	LOOP	0/0
Se2/0	6	6	10	62	P2P	0/0
Tu0	1000	0	19	11111	DOWN	0/0

インターフェイス上で認証を使用した OSPF の例

次に、インターフェイスでの認証が有効になっている `showipv6ospfinterface` コマンドの出力例を示します。

```

デバイス# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)

```

ヌル認証を使用した OSPF の例

次に、ヌル認証をインターフェイス上に設定した `showipv6ospfinterface` コマンドの出力例を示します。

```

デバイス# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)

```

エリアに認証を使用した OSPF の例

次に、エリアに認証を設定した **show ipv6 ospf interface** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)

```

ダイナミック コストを使用した OSPF の例

次に、OSPF コストダイナミックを設定した場合の **show ipv6 ospf interface** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf interface serial 2/0
Serial2/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
  Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
  Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
  Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
  Hello due in 00:00:19
  Index 1/2/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)

```

OSPF グレースフル リスタートの例

次に、OSPF グレースフルリスタート機能を設定した場合の **show ipv6 ospf interface** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3

```

```

Network Type POINT_TO_POINT, Cost: 10
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Graceful Restart p2p timeout in 00:00:19
Hello due in 00:00:02
Graceful Restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 10.1.1.1
Suppress hello for 0 neighbor(s)

```

有効化されたプロトコルの例

次に、Bidirectional Forwarding Detection (BFD) に OSPF インターフェイスが有効になっている例を示します。

```

デバイス# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 10.1.0.1
Suppress hello for 0 neighbor(s)

```

Related Commands

コマンド	説明
show ipv6 ospf graceful-restart	OSPFv3 グレースフルリスタートの情報を表示します。

show ipv6 ospf request-list

ルータが要求したすべてのリンクステートアドバタイズメントのリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf request-list** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、Open Shortest Path First (OSPF) ルーティングプロセスが有効になっているときに管理する目的で割り当てられた番号です。
<i>area-id</i>	(任意) 指定したエリアに関する情報のみを表示します。
<i>neighbor</i>	(任意) このネイバーからルータにより要求されるすべての LSA のリストを表示します。
<i>interface</i>	(任意) このインターフェイスからルータにより要求されるすべての LSA のリストを表示します。
<i>interface-neighbor</i>	(任意) このネイバーのインターフェイスのルータが要求するすべての LSA のリストを表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 ospf request-list コマンドで表示される情報は、OSPF ルーティング操作のデバッグに役立ちます。

Examples

次に、ルータが要求する LSA に関する情報の例を示します。

```

デバイス# show ipv6 ospf request-list

          OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600
Type    LS ID      ADV RTR      Seq NO      Age      Checksum
  1      0.0.0.0      192.168.255.3 0x800000C2  1       0x0014C5
  1      0.0.0.0      192.168.255.2 0x800000C8  0       0x000BCA
  1      0.0.0.0      192.168.255.1 0x800000C5  1       0x008CD1
  2      0.0.0.3      192.168.255.3 0x800000A9  774    0x0058C0
  2      0.0.0.2      192.168.255.3 0x800000B7  1       0x003A63

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 65: show ipv6 ospf request-list フィールドの説明

フィールド	説明
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	情報が表示されるルータの ID
Interface Ethernet0/0	情報が表示されるインターフェイス
Type	LSA のタイプ
LS ID	LSA のリンクステート ID。
ADV RTR	アドバタイズルータの IP アドレス
Seq NO	LSA のシーケンス番号
Age	LSA の経過時間（秒単位）
Checksum	LSA のチェックサム

show ipv6 ospf retransmission-list

再送信を待機しているすべてのリンクステートアドバタイズメントのリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf retransmission-list** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

<i>process-id</i>	(任意) 内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティングプロセスが有効になっているときに管理する目的で割り当てられた番号です。
<i>area-id</i>	(任意) 指定したエリアに関する情報のみを表示します。
<i>neighbor</i>	(任意) このネイバーの再送信を待機しているすべてのLSAのリストを表示します。
<i>interface</i>	(任意) このインターフェイスで再送信を待機しているすべてのLSAのリストを表示します。
<i>interface neighbor</i>	(任意) このネイバーからこのインターフェイスで再送信を待機しているすべてのLSAのリストを表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 ospf retransmission-list コマンドによって表示される情報は、Open Shortest Path First (OSPF) ルーティング動作のデバッグに役立ちます。

Examples

次に、**show ipv6 ospf retransmission-list** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf retransmission-list

      OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
Neighbor 192.168.255.1, interface Ethernet0/0
Link state retransmission due in 3759 msec, Queue length 1
Type   LS ID          ADV RTR          Seq NO          Age          Checksum
0x2001 0                192.168.255.2   0x80000222     1            0x00AE52

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 66: show ipv6 ospf retransmission-list フィールドの説明

フィールド	説明
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	情報が表示されるルータの ID
Interface Ethernet0/0	情報が表示されるインターフェイス
Link state retransmission due in	次のリンクステート送信までの時間
Queue length	再送信キューのエレメントの数
Type	LSA のタイプ
LS ID	LSA のリンクステート ID。
ADV RTR	アドバタイズルータの IP アドレス
Seq NO	LSA のシーケンス番号
Age	LSA の経過時間（秒単位）
Checksum	LSA のチェックサム

show ipv6 ospf statistics

Open Shortest Path First for IPv6（OSPFv6）最短パス優先（SPF）計算の統計を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf statistics** コマンドを使用します。

show ipv6 ospf statistics [detail]

Syntax Description

detail	（任意）各 OSPF エリアの統計情報を個別に表示し、追加の詳細統計情報を含めます。
---------------	--

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 ospf statistics コマンドは、SPF 計算およびそれらをトリガーするイベントに関する重要な情報を提供します。この情報は、OSPF ネットワーク メンテナンスおよびトラブルシューティングの両方に役に立ちます。たとえば、**show ipv6 ospf statistics** コマンドは、リンクステートアドバタイズメント（LSA）フラッピングのトラブルシューティングの最初のステップとして入力することをお勧めします。

Examples

次に、各 OSPFv6 エリアの詳細な統計の例を示します。

```

デバイス# show ipv6 ospf statistics detail
  Area 0: SPF algorithm executed 3 times
SPF 1 executed 00:06:57 ago, SPF type Full
SPF calculation time (in msec):
SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
0      0        0      0      0      0      0      0
RIB manipulation time (in msec):
RIB Update    RIB Delete
0              0
LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
Change record R N SN SA L
LSAs changed 1
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
10.2.2.2/0(R)
SPF 2 executed 00:06:47 ago, SPF type Full
SPF calculation time (in msec):
SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
0      0        0      0      0      0      0      0
RIB manipulation time (in msec):
RIB Update    RIB Delete
0              0
LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X7:0
Change record R L P
LSAs changed 4

```

```
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(P)
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 67: show ipv6 ospf statistics フィールドの説明

フィールド	説明
Area	OSPF エリア ID。
SPF	OSPF エリアで実行された SPF アルゴリズムの数。この数は、エリアで SPF アルゴリズムが実行されるたびに 1 つずつ増加します。
Executed ago	SPF アルゴリズムが実行されてから現在の時間までの経過時間（ミリ秒単位）。
SPF type	SPF タイプは Full または Incremental のいずれかです。
SPT	SPF アルゴリズムの最初のステージの計算（ショートパスツリーの構築）に必要な時間（ミリ秒単位）。SPT 時間とスタブネットワークのリンクの処理に必要な時間の合計が、内部時間と等しくなります。
Ext	SPF アルゴリズムが外部および Not So Stubby Area (NSSA) の LSA を処理し、外部および NSSA ルートをルーティングテーブルにインストールする時間（ミリ秒単位）。
Total	SPF アルゴリズムプロセスの合計継続時間（ミリ秒単位）。
LSIDs processed	SPF 計算中に処理された LSA の数： <ul style="list-style-type: none"> • N: ネットワークの LSA。 • R: ルータの LSA。 • SA: サマリー自律システム境界ルータ (ASBR) (SA) の LSA。 • SN: サマリーネットワーク (SN) の LSA。 • Stub: スタブリンク。 • X7: 外部タイプ 7 (X7) の LSA。

show ipv6 ospf summary-prefix

OSPF プロセスに設定されているすべてのサマリーアドレス再配布情報のリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf summary-prefix** コマンドを使用します。

show ipv6 ospf [*process-id*] **summary-prefix**

Syntax Description

<i>process-id</i>	(任意) 内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティングプロセスが有効になっているときに管理する目的で割り当てられた番号です。
-------------------	--

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

引数 *process-id* は、10 進数または IPv6 アドレス フォーマットで入力できます。

Examples

次に、**show ipv6 ospf summary-prefix** コマンドの出力例を示します。

```
デバイス# show ipv6 ospf summary-prefix
```

```
OSPFv3 Process 1, Summary-prefix  
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 68: show ipv6 ospf summary-prefix フィールドの説明

フィールド	説明
OSPFv3 Process	情報が表示されるルータのプロセス ID。
Metric	宛先ルータに到達するために使用するメトリック。
Type	リンクステートアドバタイズメント (LSA) のタイプ。
Tag	LSA タグ。

show ipv6 ospf timers rate-limit

レート制限キュー内のすべてのリンクステートアドバタイズメント (LSA) を表示するには、特権 EXEC モードで **show ipv6 ospf timers rate-limit** コマンドを使用します。

show ipv6 ospf timers rate-limit

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines キュー内の LSA がいつ送信されるかを把握するには、**show ipv6 ospf timers rate-limit** コマンドを使用します。

Examples

show ipv6 ospf timers rate-limit の出力例

次に、**show ipv6 ospf timers rate-limit** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf timers rate-limit
List of LSAs that are in rate limit Queue
  LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
  LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
  
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 69: show ipv6 ospf timers rate-limit フィールドの説明

フィールド	説明
LSAID	LSA の ID
Type	LSA のタイプ
Adv Rtr	アドバタイジング ルータの ID です。
Due in:	LSA の送信スケジュール (時:分:秒形式)

show ipv6 ospf traffic

IPv6 Open Shortest Path First バージョン 3 (OSPFv3) のトラフィック統計を表示するには、特権 EXEC モードで **show ipv6 ospf traffic** コマンドを使用します。

show ipv6 ospf [*process-id*] **traffic** [*interface-type interface-number*]

Syntax Description

<i>process-id</i>	(任意) トラフィック統計情報を必要とする OSPF プロセス ID (たとえば、キュー統計情報、OSPF プロセス下の各インターフェイスの統計情報、OSPF ごとのプロセス統計情報などです)。
<i>interface-type</i> <i>interface-number</i>	(任意) 特定の OSPF インターフェイスに関連付けられるタイプおよび番号。

Command Default

引数を指定せずに **show ipv6 ospf traffic** コマンドを入力すると、グローバル OSPF トラフィック統計が表示されます。これには、各 OSPF プロセスのキュー統計、各インターフェイスの統計、および OSPF プロセスごとの統計が含まれています。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

表示されるトラフィック統計を特定の OSPF プロセスに限定するには、引数 *process-id* に値を入力します。または、出力を OSPF プロセスに関連付けられている特定のインターフェイスのトラフィック統計に限定するには、*interface-type* 引数と *interface-number* 引数に値を入力します。カウンタをリセットし、統計情報をクリアするには、**clear ipv6 ospf traffic** コマンドを使用します。

Examples

次に、OSPFv3 の **show ipv6 ospf traffic** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf traffic
OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
  Interface Serial2/0
OSPFv3 packets received/sent

```

```

Type          Packets          Bytes
RX Invalid    0                0
RX Hello      5                196
RX DB des     4                172
RX LS req     1                52
RX LS upd     4                320
RX LS ack     2                112
RX Total      16              852
TX Failed     0                0
TX Hello      8                304
TX DB des     3                144
TX LS req     1                52
TX LS upd     3                252
TX LS ack     3                148
TX Total      18              900
OSPFv3 header errors
Length 0, Checksum 0, Version 0, No Virtual Link 0,
Area Mismatch 0, Self Originated 0, Duplicate ID 0,
Instance ID 0, Hello 0, MTU Mismatch 0,
Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
Type 0, Length 0, Data 0, Checksum 0,
Interface Ethernet0/0
OSPFv3 packets received/sent
Type          Packets          Bytes
RX Invalid    0                0
RX Hello      6                240
RX DB des     3                144
RX LS req     1                52
RX LS upd     5                372
RX LS ack     2                152
RX Total      17              960
TX Failed     0                0
TX Hello      11               420
TX DB des     9                312
TX LS req     1                52
TX LS upd     5                376
TX LS ack     3                148
TX Total      29              1308
OSPFv3 header errors
Length 0, Checksum 0, Version 0, No Virtual Link 0,
Area Mismatch 0, Self Originated 0, Duplicate ID 0,
Instance ID 0, Hello 0, MTU Mismatch 0,
Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
Type          Packets          Bytes
RX Invalid    0                0
RX Hello      11               436
RX DB des     7                316
RX LS req     2                104
RX LS upd     9                692
RX LS ack     4                264
RX Total      33              1812
TX Failed     0                0
TX Hello      19               724
TX DB des     12               456
TX LS req     2                104
TX LS upd     8                628
TX LS ack     6                296
TX Total      47              2208
OSPFv3 header errors

```

show ipv6 ospf traffic

```

Length 0, Checksum 0, Version 0, No Virtual Link 0,
Area Mismatch 0, Self Originated 0, Duplicate ID 0,
Instance ID 0, Hello 0, MTU Mismatch 0,
Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
Type 0, Length 0, Data 0, Checksum 0,

```

ネットワーク管理者は、次に示すように **clear ipv6 ospf traffic** コマンドを入力することで、新しい統計の収集、カウンタのリセット、およびトラフィック統計のクリアを開始できます。

```
デバイス# clear ipv6 ospf traffic
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 70: show ipv6 ospf traffic フィールドの説明

フィールド	説明
OSPFv3 statistics	ルータで実行されるすべての OSPF プロセスで集められたトラフィック統計情報。showiptraffic コマンドとの互換性を確保するため、チェックサムエラーのみが表示されます。ルート マップ名を識別します。
OSPFv3 queues statistic for process ID	Cisco IOS ソフトウェア固有のキュー統計。
Hello queue	パケットスイッチングコード（プロセス IP 入力）と受信したすべての OSPF パケットの OSPF hello プロセス間の内部 Cisco IOS キューの統計。
Router queue	OSPF hello プロセスと受信したすべての OSPF パケット（OSPF hello を除く）の OSPF ルータ間の内部 Cisco IOS キューの統計。
queue size	キューの実際のサイズ。
queue limit	キューの最大許容サイズ。
queue max size	キューの最大記録サイズ。
Interface statistics	指定 OSPFv3 プロセス ID に属するすべてのインターフェイスのインターフェイスごとのトラフィック統計情報。
OSPFv3 packets received/sent	パケットタイプ別にソートされた、インターフェイスで受信および送信された OSPFv3 パケットの数。
OSPFv3 header errors	パケットが OSPFv3 パケットのヘッダー エラーのために破棄された場合、そのパケットがこのセクションに表示されます。破棄されたパケットは、適切な破棄理由に従いカウントされます。
OSPFv3 LSA errors	パケットが OSPF リンクステートアドバタイズメント（LSA）のヘッダーエラーのために破棄された場合、そのパケットがこのセクションに表示されます。破棄されたパケットは、適切な破棄理由に従いカウントされます。

フィールド	説明
Summary traffic statistics for process ID	<p>OSPFv3 プロセスで集められたサマリー トラフィック統計情報。</p> <p>Note OSPFv3 プロセス ID は、設定で OSPF プロセスに割り当てられる一意な値です。</p> <p>受け取ったエラーに関する値は、グローバル OSPF 統計情報にリストされるチェックサムエラーの合計とは異なり、OSPFv3 プロセスにより検出される OSPFv3 ヘッダー エラーの合計です。</p>

Related Commands

コマンド	説明
clear ip ospf traffic	OSPFv2 トラフィック統計情報をクリアします。
clear ipv6 ospf traffic	OSPFv3 トラフィック統計情報をクリアします。
show ip ospf traffic	OSPFv2 トラフィック統計情報を表示します。

show ipv6 ospf virtual-links

Open Shortest Path First (OSPF) 仮想リンクのパラメータおよび現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 ospf virtual-links** コマンドを使用します。

show ipv6 ospf virtual-links

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 ospf virtual-links コマンドで表示される情報は、OSPF ルーティング操作のデバッグに役立ちます。

Examples

次に、**show ipv6 ospf virtual-links** コマンドの出力例を示します。

```

デバイス# show ipv6 ospf virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 71: show ipv6 ospf virtual-links フィールドの説明

フィールド	説明
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	OSPF ネイバー、およびそのネイバーとのリンクがアップまたはダウン状態であるか指定します。
Interface ID	ルータのインターフェイス ID および IPv6 アドレス。
Transit area 2	仮想リンクが形成される移行エリア。
via interface ATM3/0	仮想リンクが形成されるインターフェイス。
Cost of using 1	仮想リンクを介して OSPF ネイバーに到達するときのコスト。

フィールド	説明
Transmit Delay is 1 sec	仮想リンクの移行遅延（秒単位）。
State POINT_TO_POINT	OSPF ネイバーの状態。
Timer intervals...	リンクに設定されるさまざまなタイマー間隔。
Hello due in 0:00:06	ネイバーからの次の hello の予想時間。

次の **show ipv6 ospf virtual-links** コマンドの出力例には、2つの仮想リンクが含まれています。1つは認証によって保護されており、もう1つは暗号化によって保護されています。

```

デバイス# show ipv6 ospf virtual-links
Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
  Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial12/0, Cost of using 64
  NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
  Adjacency State FULL (Hello suppressed)
  Index 1/2/4, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
  Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial11/0, Cost of using 128
  MD5 authentication SPI 940, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Adjacency State FULL (Hello suppressed)
  Index 1/1/3, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec

```

show ipv6 pim anycast-RP

IPv6 PIM エニーキャストの RP 動作を確認するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim anycast-RP** コマンドを使用します。

show ipv6 pim anycast-RP *rp-address*

Syntax Description

<i>rp-address</i>	確認する RP アドレス。
-------------------	---------------

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Examples

デバイス# **show ipv6 pim anycast-rp 110::1:1:1**

```
Anycast RP Peers For 110::1:1:1   Last Register/Register-Stop received
20::1:1:1 00:00:00/00:00:00
```

Related Commands

コマンド	説明
ipv6 pim anycast-RP	エニーキャストグループ範囲の PIM RP のアドレスを設定します。

show ipv6 pim bsr

Protocol Independent Multicast (PIM) ブートストラップルータ (BSR) プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim bsr** コマンドを使用します。

show ipv6 pim [*vrf vrf-name*] **bsr** {*election* | *rp-cache* | *candidate-rp*}

Syntax Description	
vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
election	BSR の状態、BSR の選択、およびブートストラップ メッセージ (BSM) 関連のタイマーを表示します。
rp-cache	選択した BSR 上のユニキャスト ランデブー ポイント候補 (C-RP) のアナウンスメントから学習した C-RP キャッシュを表示します。
candidate-rp	C-RP として設定されているデバイス上の C-RP の状態を表示します。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines BSR 選択ステートマシン、C-RP アドバタイズメント ステート マシン、および C-RP キャッシュの詳細を表示するには、**show ipv6 pim bsr** コマンドを使用します。C-RP キャッシュの情報は、選択した BSR デバイス上にのみ表示され、C-RP ステートマシンの情報は C-RP として設定されているデバイス上にのみ表示されます。

Examples 次に、BSM 選択情報を表示する例を示します。

```

デバイス# show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 72: show ipv6 pim bsr election のフィールドの説明

フィールド	説明
Scope Range List	この BSR 情報を適用する範囲。
This system is the Bootstrap Router (BSR)	このデバイスが BSR であること、およびそれに関連付けられているパラメータに関する情報を表示します。
BS Timer	選択した BSR について、BS タイマーは次の BSM が発信される時間を表示します。 ドメイン内のその他すべてのデバイスについては、BS タイマーは選択した BSR の期限が切れる時間を表示します。
This system is candidate BSR	このデバイスが BSR 候補であること、およびそれに関連付けられているパラメータに関する情報を表示します。

次に、BSR でさまざまな C-RP から学習した情報を表示する例を示します。この例では、2 つの RP 候補が FF00::/8 またはデフォルトの IPv6 マルチキャストの範囲にアドバタイズメントを送信しています。

```

デバイス# show ipv6 pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
  RP 10::1:1:3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20::1:1:1
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5

```

次に、C-RP に関する情報を表示する例を示します。この RP は特定の範囲の値を指定せずに設定されているため、RP は受信した BSM を通じて学習したすべての BSR に C-RP アドバタイズメントを送信します。

```

デバイス# show ipv6 pim bsr candidate-rp
PIMv2 C-RP information
  Candidate RP: 10::1:1:3
    All Learnt Scoped Zones, Priority 192, Holdtime 150
    Advertisement interval 60 seconds
    Next advertisement in 00:00:33

```

次に、IPv6 C-BSR が PIM 対応であることを確認する例を示します。IPv6 C-BSR インターフェイスで PIM が無効になっているか、あるいは C-BSR または C-RP が PIM が有効になっていないインターフェイスのアドレスで設定されている場合、**show ipv6 pim bsr** コマンドを **election** キーワードを指定して使用すると、代わりにその情報を表示します。

```

デバイス# show ipv6 pim bsr election

PIMv2 BSR information

BSR Election Information

```

```
Scope Range List: ff00::/8
  BSR Address: 2001:DB8:1:1:2
  Uptime: 00:02:42, BSR Priority: 34, Hash mask length: 28
  RPF: FE80::20:1:2,Ethernet1/0
  BS Timer: 00:01:27
```

show ipv6 pim df

各ランデブーポイント（RP）の各インターフェイスの代表フォワーダ（DF）の選択状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim df** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*]

Syntax Description

vrf <i>vrf-name</i>	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
<i>interface-type interface-number</i>	（任意）インターフェイスタイプおよび番号詳細については、疑問符（?）オンラインヘルプ機能を使用します。
<i>rp-address</i>	（任意）RP IPv6 アドレス。

Command Default

インターフェイスまたは RP のアドレスを指定しないと、すべての DF が表示されます。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

双方向マルチキャストトラフィックが予想どおりにフローしない場合に各 Protocol Independent Multicast（PIM）対応のインターフェイスの DF の選択状態を表示するには、**show ipv6 pim df** コマンドを使用します。

Examples

次に、DF の選択状態を表示する例を示します。

```

デバイス# show ipv6 pim df
Interface          DF State      Timer          Metrics
Ethernet0/0        Winner        4s 8ms        [120/2]
  RP :200::1
Ethernet1/0        Lose          0s 0ms        [inf/inf]
  RP :200::1

```

次に、RP に関する情報を表示する例を示します。

```

デバイス# show ipv6 pim df
Interface          DF State      Timer          Metrics
Ethernet0/0        None:RP LAN  0s 0ms        [inf/inf]
  RP :200::1
Ethernet1/0        Winner        7s 600ms      [0/0]
  RP :200::1
Ethernet2/0        Winner        9s 8ms        [0/0]
  RP :200::1

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 73: show ipv6 pim df フィールドの説明

フィールド	説明
Interface	PIM を実行するように設定されているインターフェイスのタイプと番号。
DF State	<p>インターフェイスでの DF の選択状態。状態は次のいずれかになります。</p> <ul style="list-style-type: none"> • Offer • Winner • Backoff • Lose • None:RP LAN <p>None:RP LAN 状態は、RP がこの LAN に直接接続されているために、この LAN 上では DF の選択が実行されないことを示します。</p>
Timer	DF 選択タイマー。
Metrics	DF によってアナウンスされた RP へのルーティング メトリック。
RP	RP の IPv6 アドレス。

Related Commands

コマンド	説明
debug ipv6 pim df-election	PIM 双方向 DF 選択メッセージ処理のデバッグ メッセージを表示します。
ipv6 pim rp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
show ipv6 pim df winner	各 RP の各インターフェイスの DF 選択ウィナーを表示します。

show ipv6 pim group-map

IPv6 Protocol Independent Multicast (PIM) のグループマッピングテーブルを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim group-map** コマンドを使用します。

```
{show ipv6 pim [vrf vrf-name ] group-map [group-namegroup-address] | [group-rangegroup-mask]
[info-source {bsr | default | embedded-rp | static}]}
```

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。
<i>group-range</i> <i>group-mask</i>	(任意) グループの範囲のリスト。同じプレフィックス長またはマスク長のグループの範囲が含まれています。
info-source	(任意) ブートストラップルータ (BSR) やスタティック設定など、特定の送信元から学習したすべてのマッピングを表示します。
bsr	BSR を通じて学習した範囲を表示します。
default	デフォルトで有効になった範囲を表示します。
embedded-rp	組み込みランデブーポイント (RP) を通じて学習したグループの範囲を表示します。
static	スタティック設定によって有効になっている範囲を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

BSR やスタティック設定など、指定した情報源がインストールしたすべてのグループマッピングを検索するには、**show ipv6 pim group-map** コマンドを使用します。

また、このコマンドは、指定した IPv6 グループアドレスのルータがグループアドレスを使用しているグループマッピングを検索したり、グループの範囲とマスク長を指定して正確なグループマッピングエントリを検索したりするためにも使用できます。

Examples

次に、**show ipv6 pim group-map** コマンドの出力例を示します。

```

デバイス# show ipv6 pim group-map
FF33::/32*
  SSM
  Info source:Static
  Uptime:00:08:32, Groups:0
FF34::/32*
  SSM
  Info source:Static
  Uptime:00:09:42, Groups:0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 74: show ipv6 pim group-map のフィールドの説明

フィールド	説明
RP	プロトコルがスパス モードまたは bidir の場合の RP ルータのアドレス。
Protocol	<p>使用するプロトコル: スパスモード (SM)、送信元特定マルチキャスト (SSM)、リンクローカル (LL)、または NOROUTE (NO)。</p> <p>LL は、リンクローカル範囲の IPv6 アドレス範囲 (ff[0-f]2::/16) に使用されます。LL は個別のプロトコル タイプとして扱われます。これは、このような宛先アドレスで受信したパケットは転送されず、ルータがそれらを受信して処理する必要があるためです。</p> <p>NOROUTE または NO は予約された、ノードローカル範囲の IPv6 アドレス範囲 (ff[0-f][0-1]::/16) に使用されます。これらのアドレスはルーティングができないため、ルータはそれら进行处理する必要がありません。</p>
Groups	この範囲のトポロジテーブル内に存在するグループの数。
Info source	特定の送信元から学習したマッピング。この場合はスタティック設定。
Uptime	表示されたグループ マッピングの稼働時間。

次に、PIM の group-to-RP キャッシュまたは mode-mapping キャッシュに存在する BSR から学習したグループマッピングを表示する例を示します。次に、グループ マッピングを学習した BSR のアドレスと、関連付けられているタイムアウトを表示する例を示します。

```

Router# show ipv6 pim group-map info-source bsr
FF00::/8*
  SM, RP: 20::1:1:1
  RPF: Et1/0, FE80::A8BB:CCFF:FE03:C202
  Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
  Uptime: 00:19:51, Groups: 0
FF00::/8*
  SM, RP: 10::1:1:3
  RPF: Et0/0, FE80::A8BB:CCFF:FE03:C102
  Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
  Uptime: 00:19:51, Groups: 0

```

show ipv6 pim interface

Protocol Independent Multicast (PIM) に設定されているインターフェイスに関する情報を表示するには、特権 EXEC モードで **show ipv6 pim interface** コマンドを使用します。

show ipv6 pim [*vrf vrf-name*] **interface** [*state-on*] [*state-off*] [*type number*]

Syntax Description

vrf vrf-name	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
state-on	(任意) PIM がイネーブルになっているインターフェイスを表示します。
state-off	(任意) PIM がディセーブルになっているインターフェイスを表示します。
type number	(任意) インターフェイス タイプおよび番号

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Usage Guidelines

PIM がインターフェイスで有効になっているかどうか、およびネイバーの数とインターフェイス上の代表ルータ (DR) を確認するには、**show ipv6 pim interface** コマンドを使用します。

Examples

次に、**show ipv6 pim interface** コマンドで **state-on** キーワードを指定した場合の出力例を示します。

```

デバイス# show ipv6 pim interface state-on
Interface          PIM Nbr Hello DR
                  Count Intvl Prior
Ethernet0         on  0   30   1
  Address:FE80::208:20FF:FE08:D7FF
  DR      :this system
POS1/0            on  0   30   1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
POS4/0           on  1   30   1
  Address:FE80::208:20FF:FE08:D554
  DR      :FE80::250:E2FF:FE8B:4C80
POS4/1           on  0   30   1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
Loopback0        on  0   30   1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 75: show ipv6 pim interface フィールドの説明

フィールド	説明
Interface	PIM を実行するように設定されているインターフェイスのタイプと番号。
PIM	インターフェイス上で PIM が有効になっているかどうか。
Nbr Count	このインターフェイスを通じて検出された PIM ネイバーの数。
Hello Intvl	PIM の hello メッセージの頻度（秒単位）。
DR	ネットワーク上の代表ルータ（DR）の IP アドレス。
Address	ネクストホップルータのインターフェイス IP アドレス。

次に、パッシブインターフェイス情報を表示するように変更した **show ipv6 pim interface** コマンドの出力例を示します。

```
デバイス(config)# show ipv6 pim interface gigabitEthernet0/0/0
```

```

Interface                PIM  Nbr  Hello  DR  BFD
                        Count Intvl Prior
GigabitEthernet0/0/0    on/P  0    30    1  On
  Address: FE80::A8BB:CCFF:FE00:9100
  DR      : this system

```

次の表で、この出力に表示される重要な変更事項を説明します。

Table 76: show ipv6 pim interface フィールドの説明

フィールド	説明
PIM	インターフェイス上で PIM が有効になっているかどうか。PIM パッシブモードを使用している場合、出力に「P」が表示されます。

Related Commands

Command	Description
show ipv6 pim neighbor	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。

show ipv6 pim join-prune statistic

各インターフェイスについて最近集約された 1,000 個、10,000 個、および 50,000 個のパケットの平均 join-prune 集約を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim join-prune statistic** コマンドを使用します。

show ipv6 pim [vrf vrf-name] join-prune statistic [interface-type]

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>interface-type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Protocol Independent Multicast (PIM) が複数の join と prune を同時に送信する場合は、それらを単一のパケットに集約します。 **show ipv6 pim join-prune statistic** コマンドは、それまでの 1,000 個の PIM join-prune パケット、それまでの 10,000 個の PIM join-prune パケット、およびそれまでの 50,000 個の PIM join-prune パケットにわたって単一のパケットに集約した join と prune の平均数を表示します。

Examples

次に、イーサネット インターフェイス 0/0/0 での join/prune 集約の例を示します。

```

デバイス# show ipv6 pim join-prune statistic Ethernet0/0/0
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted          Received
Ethernet0/0/0      0 / 0 / 0           1 / 0 / 0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 77: show ipv6 pim join-prune statistics フィールドの説明

フィールド	説明
Interface	指定したパケットを送信するインターフェイス、または指定したパケットを受信するインターフェイス。
Transmitted	このインターフェイスで送信したパケットの数。

フィールド	説明
Received	このインターフェイスで受信したパケットの数。

show ipv6 pim limit

Protocol Independent Multicast (PIM) インターフェイスの制限を表示するには、特権 EXEC モードで **show ipv6 pim limit** コマンドを使用します。

```
show ipv6 pim [vrf vrf-name ] limit [interface]
```

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>interface</i>	(任意) 制限情報が提供される特定のインターフェイス。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 pim limit コマンドはインターフェイス統計の制限を確認します。オプションの引数 *interface* を有効にすると、指定したインターフェイスの情報のみが表示されます。

Examples

次に、PIM インターフェイスの制限情報を表示する例を示します。

```
デバイス# show ipv6 pim limit
```

Related Commands

コマンド	説明
ipv6 multicast limit	IPv6 のインターフェイス単位の mroute ステートリミッタを設定します。
ipv6 multicast limit cost	IPv6 のインターフェイスごとの mroute ステートリミッタと一致する mroute にコストを適用します。

show ipv6 pim neighbor

Cisco ソフトウェアが検出した Protocol Independent Multicast (PIM) ネイバーを表示するには、特権 EXEC モードで **show ipv6 pim neighbor** コマンドを使用します。

show ipv6 pim [*vrf vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**]

Syntax Description	
vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
detail	(任意) ルーティング可能なアドレス hello オプションを通じて学習したネイバーがある場合は、そのネイバーの追加アドレスを表示します。
<i>interface-type</i> <i>interface-number</i>	(任意) インターフェイス タイプおよび番号
count	(任意) 各インターフェイスのネイバー カウントを表示します。

Command Modes 特権 EXEC (#)

Command History	
リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **Show ipv6 pim neighbor** コマンドは、PIM 用に設定されている LAN 上のルータを表示します。

Examples

次に、**show ipv6 pim neighbor** コマンドで **detail** キーワードを指定して、ルーティング可能なアドレスの hello オプションを通して学習されたネイバーの追加アドレスを識別する場合の出力例を示します。

デバイス# **show ipv6 pim neighbor detail**

```
Neighbor Address(es)      Interface      Uptime      Expires DR pri Bidir
FE80::A8BB:CCFF:FE00:401  Ethernet0/0   01:34:16   00:01:16 1      B
60::1:1:3
FE80::A8BB:CCFF:FE00:501  Ethernet0/0   01:34:15   00:01:18 1      B
60::1:1:4
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 78: show ipv6 pim neighbor フィールドの説明

フィールド	説明
Neighbor addresses	PIM ネイバーの IPv6 アドレス。

show ipv6 pim neighbor

フィールド	説明
Interface	ネイバーに到達可能なインターフェイスのタイプと番号
Uptime	PIM ネイバー テーブル内にエントリが存在する時間（時間、分、秒）。
Expires	IPv6 マルチキャストルーティングテーブルからエントリが削除されるまでの期間（時間、分、秒）。
DR	このネイバーが LAN の代表ルータ（DR）であることを示します。
pri	このネイバーが使用する DR の優先順位。
Bidir	ネイバーは双方向モードで PIM に対応します。

Related Commands

コマンド	説明
show ipv6 pim interfaces	PIM に対して設定されたインターフェイスに関する情報を表示します。

show ipv6 pim range-list

IPv6 マルチキャストの範囲のリストに関する情報を表示するには、特権 EXEC モードで **show ipv6 pim range-list** コマンドを使用します。

```
show ipv6 pim [vrf vrf-name] range-list [config] [rp-address|rp-name]
```

Syntax Description	
vrf vrf-name	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
config	(任意) クライアント。ルータで設定されている範囲のリストを表示します。
rp-address rp-name	(任意) Protocol Independent Multicast (PIM) ランデブーポイント (RP) のアドレス。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ipv6 pim range-list** コマンドは、クライアントごとおよびモードごとに IPv6 マルチキャストの範囲のリストを表示します。クライアントは、指定した範囲のリストの学習元のエンティティです。クライアントは **config**、モードは 送信元特定マルチキャスト (SSM) モードまたはスパスモードである場合があります。

Examples

次に、**show ipv6 pim range-list** コマンドの出力例を示します。

```
デバイス# show ipv6 pim range-list
config SSM Exp:never Learnt from :::
FF33::/32 Up:00:26:33
FF34::/32 Up:00:26:33
FF35::/32 Up:00:26:33
FF36::/32 Up:00:26:33
FF37::/32 Up:00:26:33
FF38::/32 Up:00:26:33
FF39::/32 Up:00:26:33
FF3A::/32 Up:00:26:33
FF3B::/32 Up:00:26:33
FF3C::/32 Up:00:26:33
FF3D::/32 Up:00:26:33
FF3E::/32 Up:00:26:33
FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
FF09::/64 Up:00:03:50
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 79: show ipv6 pim range-list フィールドの説明

フィールド	説明
config	Config がクライアントです。
SSM	使用中のプロトコル。
FF33::/32	グループの範囲。
Up:	稼働時間。

show ipv6 pim topology

特定のグループまたはすべてのグループの Protocol Independent Multicast (PIM) トポロジテーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim topology** コマンドを使用します。

```
show ipv6 pim [vrf vrf-name] topology [group-name | group-address [source-addresssource-name]]
| link-local] route-count [detail]
```

Syntax Description

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。
<i>source-address</i> <i>source-name</i>	(任意) 送信元の IPv6 アドレスまたは名前。
link-local	(任意) リンク ローカル グループを表示します。
route-count	(任意) PIM トポロジテーブル内のルートの数を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、指定したグループ (*, G)、(S, G)、(S, G) ランデブー ポイント ツリー (RPT)) を PIM トポロジテーブルに内部的に格納したとおりに表示します。PIM トポロジテーブルには、指定したグループのさまざまなエントリが含まれており、それぞれが固有のインターフェイス リストを備えている場合があります。結果の転送状態が Multicast Routing Information Base (MRIB) テーブルに保持されます。このテーブルは、データ パケットを承認するインターフェイスと、データ パケットを指定した (S, G) エントリに転送するインターフェイスが示されています。また、転送時にはマルチキャスト転送情報ベース (MFIB) テーブルを使用して、パケットごとの転送アクションを決定します。

route-count キーワードは、リンクローカルエントリを含めて、すべてのエントリのカウントを表示します。

PIM は、これらのエントリの内容を MRIB を通じてやり取りします。MRIB は、PIM などのマルチキャストルーティングプロトコルと、マルチキャストリスナー検出 (MLD) などのローカルメンバーシッププロトコルとの通信における仲介手段であり、システムのマルチキャスト転送エンジンです。

たとえば、MLD レポートまたは PIM (*, G) join メッセージの受信時にインターフェイスが PIM トポロジテーブルの (*, G) エントリに追加されるとします。同様に、S と G の MLD INCLUDE レポートまたは PIM (S, G) join メッセージの受信時にインターフェイスが (S, G) エントリに追加されるとします。次に、PIM が (S, G) エントリを immediate olist ((S, G) から) および inherited olist ((*, G) から) で MRIB にインストールします。そのため、指定したエントリ (S, G) の正しいフローディング ステータスは、PIM トポロジテーブルではなく、MRIB または MFIB でのみ確認できます。

Examples

次に、`show ipv6 pim topology` コマンドの出力例を示します。

```

デバイス# show ipv6 pim topology
IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
             RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
             RR - Register Received, SR - Sending Registers, E - MSDP External,
             DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
                II - Internal Interest, ID - Internal Dissinterest,
                LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:40::1:1:2
RPF:Ethernet1/1,FE81::1
   Ethernet0/1          02:26:56   fwd LI LH
(50::1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
   Ethernet1/1          00:00:07   off LI

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 80: show ipv6 pim topology フィールドの説明

フィールド	説明
Entry flags: KAT	送信元が起動している間の2つの間隔を追跡するには、送信元に関連付けられているキープアライブ タイマー (KAT) を使用します。送信元が最初にアクティブに時点で、ファーストホップ ルータがキープアライブ タイマーを3分30秒に設定します。その間は送信元が起動しているかどうかを確認するためのプローブは行いません。このタイマーが満了すると、ルータはプローブ間隔を開始し、タイマーを65秒にリセットします。その間、ルータは送信元が起動していると想定し、実際にそうであるかどうかを判断するためのプローブを開始します。ルータが送信元は起動していると判断すると、ルータはプローブ間隔を終了し、キープアライブ タイマーを3分30秒にリセットします。送信元が起動していない場合は、プローブ間隔の終了時点でエントリが削除されます。
AA, PA	ルータが特定の送信元のプローブ間隔に入っているときに、推定アライブ (AA) フラグとプローブアライブ (PA) フラグが設定されます。

フィールド	説明
RR	RP が送信元の代表ルータ (DR) から登録を受信し、送信元の状態を ルートプロセッサ上で alive に保っている限り、登録受信済み (RR) フラグがルートプロセッサ (RP) の (S, G) エントリ上に設定されます。
SR	DR が RP に登録を送信している限り、送信側登録 (SR) フラグが DR 上の (S, G) エントリ上に設定されます。

Related Commands

コマンド	説明
show ipv6 mrib client	MRIB のクライアントに関する情報を表示します。
show ipv6 mrib route	MRIB ルート情報を表示します。

show ipv6 pim traffic

Protocol Independent Multicast (PIM) トラフィックカウンタを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim traffic** コマンドを使用します。

show ipv6 pim [vrf vrf-name] traffic

Syntax Description

vrf vrf-name	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
---------------------	--

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

予測した数の PIM プロトコルメッセージを送受信したかどうかを確認するには、**show ipv6 pim traffic** コマンドを使用します。

Examples

次に、送受信された PIM プロトコルメッセージの数を表示する例を示します。

```

デバイス# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

```

	Received	Sent
Valid PIM Packets	22	22
Hello	22	22
Join-Prune	0	0
Register	0	0
Register Stop	0	0
Assert	0	0
Bidir DF Election	0	0
Errors:		
Malformed Packets		0
Bad Checksums		0
Send Errors		0
Packet Sent on Loopback Errors		0
Packets Received on PIM-disabled Interface		0
Packets Received with Unknown PIM Version		0

次の表で、この出力に表示される重要なフィールドを説明します。

Table 81: show ipv6 pim traffic フィールドの説明

フィールド	説明
Elapsed time since counters cleared	カウンタをクリアしてからの時間を示します（時間、分、秒単位）。
Valid PIM Packets	送受信した有効な PIM パケットの数。
Hello	送受信した有効な hello メッセージの数。
Join-Prune	送受信した join アナウンスメントと prune アナウンスメントの数。
Register	送受信した PIM register メッセージの数。
Register Stop	送受信した PIM register stop メッセージの数。
Assert	送受信したアサートの数。

show ipv6 pim tunnel

インターフェイス上の Protocol Independent Multicast (PIM) 登録カプセル化トンネルおよびカプセル化解除トンネルを表示するには、特権 EXEC モードで **show ipv6 pim tunnel** コマンドを使用します。

show ipv6 pim [**vrf vrf-name**] **tunnel** [*interface-type interface-number*]

Syntax Description

vrf vrf-name	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
interface-type interface-number	(任意) トンネル インターフェイスのタイプおよび番号

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

オプションの *interface* キーワードを指定せずに **show ipv6 pim tunnel** コマンドを使用すると、PIM 登録カプセル化トンネルインターフェイスとカプセル化解除トンネルインターフェイスに関する情報が表示されます。

PIM カプセル化トンネルは、レジスタ トンネルです。カプセル化トンネルは、各ルータ上のすべての既知のランデブーポイント (RP) に対して作成されます。PIM カプセル化解除トンネルは、レジスタ カプセル化解除トンネルです。カプセル化解除トンネルは、RP アドレスとして設定されているアドレスの RP に作成されます。

Examples

次に、RP での **show ipv6 pim tunnel** コマンドの出力例を示します。

```

デバイス# show ipv6 pim tunnel
Tunnel0*
  Type   :PIM Encap
  RP     :100::1
  Source:100::1
Tunnel0*
  Type   :PIM Decap
  RP     :100::1
  Source: -

```

次に、RP 以外での **show ipv6 pim tunnel** コマンドの出力例を示します。

```

デバイス# show ipv6 pim tunnel
Tunnel0*
  Type   :PIM Encap
  RP     :100::1
  Source:2001::1:1:1

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 82: `show ipv6 pim tunnel` フィールドの説明

フィールド	説明
Tunnel0*	トンネルの名前。
Type	トンネルのタイプ。PIM のカプセル化または PIM カプセル化の解除ができます。
source	RP にカプセル化登録を送信しているルータの送信元アドレス。

show ipv6 policy

IPv6 ポリシーベースルーティング（PBR）設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 policy** コマンドを使用します。

show ipv6 policy

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IPv4 の場合と同じように、ルート マップ上で IPv6 ポリシーの一致がカウントされます。そのため、IPv6 ポリシーの一致も **show route-map** コマンドで表示できます。

Examples

次に、PBR 設定を表示する例を示します。

```
デバイス# show ipv6 policy
```

```
Interface          Routemap
Ethernet0/0        src-1
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
Interface	Protocol-Independent Multicast（PIM）を実行するように設定されているインターフェイスのタイプと番号。
Routemap	IPv6 ポリシーの一致がカウントされたルート マップの名前。

Related Commands

コマンド	説明
show route-map	設定されたすべてのルート マップ、または指定した 1 つのルート マップだけを表示します。

show ipv6 prefix-list

IPv6 プレフィックスリストまたは IPv6 プレフィックスリストのエントリに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 prefix-list** コマンドを使用します。

```
show ipv6 prefix-list [detail | summary] [list-name]
show ipv6 prefix-list list-name ipv6-prefix/prefix-length [longer | first-match]
show ipv6 prefix-list list-name seq seq-num
```

Syntax Description	detail summary	(任意) すべての IPv6 プレフィックス リストに関する詳細情報または要約情報を表示します。
	<i>list-name</i>	(任意) 特定の IPv6 プレフィックス リストの名前。
	<i>ipv6-prefix</i>	指定した IPv6 ネットワークのすべてのプレフィックス リスト エントリ。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
	<i>/ prefix-length</i>	IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
	longer	(任意) 指定した <i>ipv6-prefix / prefix-length</i> values よりも詳細に IPv6 プレフィックスリストのすべてのエントリを表示します。
	first-match	(任意) 指定した <i>ipv6-prefix / prefix-length</i> の値と一致する IPv6 プレフィックスリストのエントリを表示します。
	seq seq-num	IPv6 プレフィックス リスト エントリのシーケンス番号。

Command Default すべての IPv6 プレフィックス リストに関する情報を表示します。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ipv6 prefix-list** コマンドは、IPv6 専用である点を除き、**show ip prefix-list** コマンドと同様の出力を提供します。

Examples

次に、**show ipv6 prefix-list** コマンドで **detail** キーワードを指定した場合の出力例を示します。

```

デバイス# show ipv6 prefix-list detail
ipv6 prefix-list 6to4:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
  seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
  count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
  seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
  seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 83: show ipv6 prefix-list フィールドの説明

フィールド	説明
Prefix list with the latest deletion/insertion:	最後に変更されたプレフィックス リスト。
count	リスト内のエントリの数。
range entries	範囲が一致するエントリの数。
sequences	プレフィックス エントリのシーケンス番号。
refcount	このプレフィックス リストを現在使用しているオブジェクトの数。
seq	リスト内のエントリ番号。
permit, deny	ステータスの付与。
hit count	プレフィックス エントリの一致の数。

次に、**show ipv6 prefix-list** コマンドで **summary** キーワードを指定した場合の出力例を示します。

```

デバイス# show ipv6 prefix-list summary
ipv6 prefix-list 6to4:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
  count: 2, range entries: 2, sequences: 5 - 10, refcount: 30

```

Related Commands

コマンド	説明
clear ipv6 prefix-list	プレフィックス リスト エントリのヒット カウントをリセットします。
distribute-list in	アップデートで受信するネットワークをフィルタリングします。

コマンド	説明
distribute-list out	ネットワークが更新時にアドバタイズされないようにします。
ipv6 prefix-list	IPv6 プレフィックス リストのエントリを作成します。
ipv6 prefix-list description	IPv6 プレフィックス リストのテキスト説明を追加します。
match ipv6 address	プレフィックス リストによって許可されるプレフィックスを持つ IPv6 ルートを配信します。
remark (prefix-list)	プレフィックス リストのエントリにコメントを追加します。

show ipv6 protocols

アクティブな IPv6 ルーティング プロトコル プロセスのパラメータおよび現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 protocols** コマンドを使用します。

show ipv6 protocols [summary]

Syntax Description

summary	(任意) 設定されているルーティング プロトコル プロセスの名前を表示します。
----------------	---

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 protocols コマンドにより表示される情報は、ルーティング動作のデバッグに役立ちます。

Examples

次に、Intermediate System-to-Intermediate System (IS-IS) ルーティングプロトコル情報を表示する **show ipv6 protocols** コマンドの出力例を示します。

```

デバイス# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16 advertised with metric 0
    L2: 44::/16 advertised with metric 20
    L2: 66::/16 advertised with metric 10
    L2: 77::/16 advertised with metric 10

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 84: IS-IS プロトコルの場合の *show ipv6 protocols* フィールドの説明

フィールド	説明
IPv6 Routing Protocol is	使用した IPv6 ルーティングプロトコルを指定します。
Interfaces	IPv6 IS-IS が設定されているインターフェイスを指定します。
Redistribution	再配布されているプロトコルのリストを表示します。
Inter-area redistribution	他のレベルに再配布されている IS-IS レベルのリストを表示します。
using prefix-list	エリア間の再配布で使用されたプレフィックスリストを指定します。
[Address Summarization]	すべてのサマリープレフィックスのリストを表示します。サマリープレフィックスがアドバタイズされている場合、後ろに「advertised with metric x」が表示されます。

show ipv6 rip

現在の IPv6 Routing Information Protocol (RIP) プロセスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 rip** コマンドを使用します。

show ipv6 rip [*name*] [**vrf** *vrf-name*] [**database** | **next-hops**]

show ipv6 rip [*name*] [**database** | **next-hops**]

Syntax Description

name	(任意) RIP プロセスの名前。名前を入力しないと、設定されているすべての RIP プロセスの詳細が表示されます。
vrf vrf-name	(任意) 指定された仮想ルーティング/転送 (VRF) インスタンスに関する情報を表示します。
database	(任意) 指定した RIP IPv6 ルーティングテーブル内のエントリに関する情報を表示します。
next-hops	(任意) 指定した RIP IPv6 プロセスのネクストホップアドレスに関する情報を表示します。RIP プロセス名を指定しないと、すべての RIP IPv6 プロセスのネクストホップアドレスが表示されます。

Command Default

現在のすべての IPv6 RIP プロセスに関する情報を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**show ipv6 rip** コマンドの出力例を示します。

```

デバイス# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
  Administrative distance is 25. Maximum paths is 4
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 8883, trigger updates 2
  Interfaces:
    Ethernet2
  Redistribution:
RIP process "two", port 521, multicast-group FF02::9, pid 61
  Administrative distance is 120. Maximum paths is 4

```

```

Updates every 30 seconds, expire after 180
Holddown lasts 0 seconds, garbage collect after 120
Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 8883, trigger updates 0
Interfaces:
None
Redistribution:

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 85: show ipv6 rip フィールドの説明

フィールド	説明
RIP process	RIP プロセスの名前。
port	RIP プロセスが使用しているポート。
multicast-group	RIP がメンバとなっている IPv6 マルチキャストグループ。
pid	RIP プロセスに割り当てられているプロセス識別番号 (pid)。
Administrative distance	ルーティング情報の送信元の優先度のランク付けに使用されます。接続されているルータにアドミニストレーティブ ディスタンス 1 があり、より大きなアドミニストレーティブ ディスタンス値を持つプロトコルによって学習されたルータよりも優先されます。
Updates	更新タイマーの値 (秒単位)。
expire	更新の期限が切れる間隔 (秒単位)。
Holddown	ホールドダウン タイマーの値 (秒単位)。
garbage collect	ガーベッジコレクション タイマーの値 (秒単位)。
Split horizon	スプリット ホライズン状態は on か off のいずれかです。
poison reverse	ポイズン リバース状態は on か off のいずれかです。
Default routes	RIP へのデフォルト ルートの起点。デフォルト ルートを生成するか、しないかです。
Periodic updates	更新タイマーに送信した RIP アップデート パケットの数。
trigger updates	トリガーされた更新として送信された RIP アップデート パケットの数。

次に、**show ipv6 rip database** コマンドの出力例を示します。

```

デバイス# show ipv6 rip one database

```

```

RIP process "one", local RIB
2001:72D:1000::/64, metric 2
Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs

```

```

2001:72D:2000::/64, metric 2, installed
  Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
2001:72D:3000::/64, metric 2, installed
  Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
  Ethernet1/2001:DB8::1, expires in 120 secs
2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
  Ethernet2/2001:DB8:0:ABCD::1
3004::/64, metric 2 tag 2A, installed
  Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 86: show ipv6 rip database フィールドの説明

フィールド	説明
RIP process	RIP プロセスの名前。
2001:72D:1000::/64	IPv6 ルートプレフィックス。
metric	ルートのメトリック。
installed	ルートが IPv6 ルーティングテーブルにインストールされています。
Ethernet2/2001:DB8:0:ABCD::1	IPv6 ルートが学習されたインターフェイスおよび LL ネクストホップ。
expires in	ルートの期限が切れるまでの間隔（秒単位）。
advertise	期限切れのルートについて、そのルートが期限切れとアドバタイズされる時間の値（秒単位）。
hold	ホールドダウンタイマーの値（秒単位）。
tag	ルートタグ。

次に、**show ipv6 rip next-hops** コマンドの出力例を示します。

```

デバイス# show ipv6 rip one next-hops

RIP process "one", Next Hops
  FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
  FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 87: show ipv6 rip next-hops フィールドの説明

フィールド	説明
RIP process	RIP プロセスの名前。

フィールド	説明
2001:DB8:0:1::1/Ethernet4/2	<p>ネクストホップアドレスおよびそれを学習したインターフェイス。ネクストホップは、ルートを学習した IPv6 RIP ネイバーのアドレスか、または IPv6 RIP アドバタイズメントで受信した明示的なネクストホップのいずれかです。</p> <p>Note IPv6 RIP ネイバーが明示的なネクストホップを使用してそのネイバーのすべてのルータをアドバタイズすることがあります。この場合、ネイバーのアドレスはネクストホップの表示に表示されません。</p>
[1 routes]	指定したネクストホップを使用している IPv6 RIP ルーティングテーブル内のルートの数。

次に、**show ipv6 rip vrf** コマンドの出力例を示します。

デバイス# **show ipv6 rip vrf red**

```
RIP VRF "red", port 521, multicast-group 2001:DB8::/32, pid 295
Administrative distance is 120. Maximum paths is 16
Updates every 30 seconds, expire after 180
Holddown lasts 0 seconds, garbage collect after 120
Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 99, trigger updates 3
Full Advertisement 0, Delayed Events 0
Interfaces:
  Ethernet0/1
  Loopback2
Redistribution:
  None
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 88: show ipv6 rip vrf フィールドの説明

フィールド	説明
RIP VRF	RIP VRF の名前。
port	RIP プロセスが使用しているポート。
multicast-group	RIP がメンバとなっている IPv6 マルチキャストグループ。
Administrative distance	ルーティング情報の送信元の優先度のランク付けに使用されます。接続されているルータにアドミニストレーティブ ディスタンス 1 があり、より大きなアドミニストレーティブ ディスタンス値を持つプロトコルによって学習されたルータよりも優先されます。
Updates	更新タイマーの値（秒単位）。
expires after	更新の期限が切れる間隔（秒単位）。

フィールド	説明
Holddown	ホールドダウン タイマーの値（秒単位）。
garbage collect	ガーベッジコレクション タイマーの値（秒単位）。
Split horizon	スプリット ホライズン状態は on か off のいずれかです。
poison reverse	ポイズン リバース状態は on か off のいずれかです。
Default routes	RIP へのデフォルト ルートの起点。デフォルト ルートを生成するか、しないかです。
Periodic updates	更新タイマーに送信した RIP アップデート パケットの数。
trigger updates	トリガーされた更新として送信された RIP アップデート パケットの数。

次に、**show ipv6 rip vrf next-hops** コマンドの出力例を示します。

```
Device# show ipv6 rip vrf blue next-hops

RIP VRF "blue", local RIB
  AAAA::/64, metric 2, installed
  Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00, expires in 177 secs
```

Table 89: show ipv6 rip vrf next-hops フィールドの説明

フィールド	説明
RIP VRF	RIP VRF の名前。
metric	ルートのメトリック。
installed	ルートが IPv6 ルーティング テーブルにインストールされています。
Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00	ネクストホップアドレスおよびそれを学習したインターフェイス。ネクストホップは、ルートを学習した IPv6 RIP ネイバーのアドレスか、または IPv6 RIP アドバタイズメントで受信した明示的なネクストホップのいずれかです。 Note IPv6 RIP ネイバーが明示的なネクストホップを使用してそのネイバーのすべてのルータをアドバタイズすることがあります。この場合、ネイバーのアドレスはネクストホップの表示に表示されません。
expires in	ルートの期限が切れるまでの間隔（秒単位）。

次に、**show ipv6 rip vrf database** コマンドの出力例を示します。

デバイス# **show ipv6 rip vrf blue database**

```
RIP VRF "blue", Next Hops
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]
```

Table 90: show ipv6 rip vrf database フィールドの説明

フィールド	説明
RIP VRF	RIP VRF の名前。
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0	IPv6 ルートが学習されたインターフェイスおよび LL ネットホップ。
1 paths	ルーティングテーブル内に存在するこのルータへの固有のパスの数を示します。

Related Commands

コマンド	説明
clear ipv6 rip	IPv6 RIP ルーティングテーブルからルートを削除します。
debug ipv6 rip	IPv6 RIP ルーティングテーブルの現在の内容を表示します。
ipv6 rip vrf-mode enable	IPv6 RIP の VRF 認識型サポートを有効にします。

show ipv6 routers

オンリンクデバイスから受信した IPv6 ルータアドバタイズメント (RA) 情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 routers** コマンドを使用します。

show ipv6 routers [*interface-type interface-number*][**conflicts**][**vrf vrf-name**][**detail**]

Syntax Description

<i>interface -type</i>	(任意) インターフェイス タイプを指定します。
<i>interface -number</i>	(任意) インターフェイス番号を指定します。
conflicts	(任意) 指定したインターフェイスに設定されている RA とは異なる RA を表示します。
vrf vrf-name	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
detail	(任意) デフォルトのデバイスとして選択するためのネイバーの資格に関する詳細を提供します。

Command Default

インターフェイスを指定しないと、すべてのインターフェイス タイプのオンリンク RA 情報が表示されます (用語 *onl-ink* は、リンク上のローカルで到達可能なアドレスのことです)。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

RAを受信するインターフェイスに設定されている RA パラメータとは異なるパラメータをアドバタイズするデバイスに **conflicting** というマークが付けられます。

Examples

次に、IPv6 インターフェイスタイプおよび番号を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
デバイス# show ipv6 routers
```

```
Device FE80::83B3:60A4 on Tunnel5, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
  Valid lifetime -1, preferred lifetime -1
Device FE80::290:27FF:FE8C:B709 on Tunnel57, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

次に、デフォルト デバイスの高いプリファレンスをアドバタイズし、このリンク上でモバイル IPv6 ホーム エージェントとして機能している単一の隣接デバイスの出力例を示します。

デバイス# **show ipv6 routers**

```
IPV6 ND Routers (table: default)
  Device FE80::100 on Ethernet0/0, last update 0 min
  Hops 64, Lifetime 50 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=1, Preference=High
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2001::100/64 onlink autoconfig
  Valid lifetime 2592000, preferred lifetime 604800
```

次の表に、この出力で表示される重要なフィールドについて説明します。

Table 91: show ipv6 routers フィールドの説明

フィールド	説明
Hops	RA に設定されているホップ制限値。
Lifetime	RA に設定されているライフタイム値。値 0 は、デバイスがデフォルトのデバイスではないことを示します。0 以外の値は、そのデバイスがデフォルトのデバイスであることを示します。
AddrFlag	値が 0 の場合は、デバイスから受信した RA はアドレスがステートフル自動設定メカニズムを使用して設定されていないことを示します。値が 1 の場合は、このメカニズムを使用してアドレスが設定されています。
OtherFlag	値が 0 の場合は、デバイスから受信した RA がアドレス以外の情報はステートフル自動設定メカニズムを使用して取得されていないことを示します。値が 1 の場合は、このメカニズムを使用してその他の情報が取得されています（値 OtherFlag は、AddrFlag の値が 1 の場合にのみ、1 になります）。
MTU	最大伝送単位（MTU）。
HomeAgentFlag=1	値は 0 または 1 のいずれかです。値 1 は、RA を受信するデバイスがこのリンク上でモバイル IPv6 ホーム エージェントとして機能していることを示し、値 0 はこのリンク上でモバイル IPv6 ホーム エージェントとして機能していないことを示します。
Preference=High	DRP 値（High、Medium、または Low のいずれか）。
Retransmit time	設定されている RetransTimer 値。ネイバー送信要求伝送用のこのリンクで使用する時間値。これは、アドレス解決と近隣到達不能検出に使用されます。値 0 は、アドバタイジング デバイスによってこの時間値が指定されていないことを意味します。
Prefix	デバイスによってアドバタイズされたプレフィックス。また、RA メッセージ内に on-link ビットまたは autoconfig ビットが設定されたかどうかを示します。

フィールド	説明
Valid lifetime	アドバタイズメントが送信された時間を基準にして、オンリンク判定のためにプレフィックスが有効である時間（秒単位）。値 -1（すべて 1、0xffffffff）は無限を意味します。
preferred lifetime	アドバタイズメントが送信された時間を基準にし、アドレスの自動設定を介してプレフィックスから生成されたアドレスが有効なままになる時間（秒単位）。値 -1（すべて 1、0xffffffff）は無限を意味します。

interface-type 引数と *interface-number* 引数を指定すると、その特定のインターフェイスに関する RA の詳細が表示されます。次に、インターフェイスタイプおよび番号を指定して入力した **show ipv6 routers** コマンドの出力例を示します。

デバイス# **show ipv6 routers tunnel 5**

```
Device FE80::83B3:60A4 on Tunnel5, last update 5 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
  Valid lifetime -1, preferred lifetime -1
```

show ipv6 routers コマンドと **conflicts** キーワードを入力すると、アドバタイズメントを受信するインターフェイスに設定されているパラメータとは異なるアドバタイジングパラメータのデバイスに関する情報が表示されます。次に、この出力例を示します。

デバイス# **show ipv6 routers conflicts**

```
Device FE80::203:FDFE:FE34:7039 on Ethernet1, last update 1 min, CONFLICT
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2003::/64 onlink autoconfig
  Valid lifetime -1, preferred lifetime -1
Device FE80::201:42FF:FECA:A5C on Ethernet1, last update 0 min, CONFLICT
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2001::/64 onlink autoconfig
  Valid lifetime -1, preferred lifetime -1
```

detail キーワードを使用すると、デバイスの優先ランク、デフォルトのデバイスとして選択されるための資格、およびデバイスが選択されたことがあるかないかに関する情報が表示されます。

デバイス# **show ipv6 routers detail**

```
Device FE80::A8BB:CCFF:FE00:5B00 on Ethernet0/0, last update 0 min
  Rank 0x811 (elegant), Default Router
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=0, Preference=Medium, trustlevel = 0
  Reachable time 0 (unspecified), Retransmit time 0 (unspecified)
  Prefix 2001::/64 onlink autoconfig
  Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 rpf

指定したユニキャストホストアドレスとプレフィックスのリバースパスフォワーディング（RPF）情報を確認するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 rpf** コマンドを使用します。

```
show ipv6 rpf {source-vrf [access-list] | vrf receiver-vrf {source-vrf [access-list] | select}}
```

Syntax Description

<i>source-vrf</i>	ルックアップが実行される Virtual Routing and Forwarding（VRF）の名前またはアドレス。
<i>receiver-vrf</i>	ルックアップを開始する VRF の名前またはアドレス。
<i>access-list</i>	グループベースの VRF 選択ポリシーに適用するアクセスコントロールリスト（ACL）の名前またはアドレス。
vrf	VRF インスタンスに関する情報を表示します。
select	グループから VRF へのマッピング情報を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 rpf コマンドは、IPv6 マルチキャストルーティングがリバースパスフォワーディング（RPF）をどのように実行したかに関する情報を表示します。ルータは複数のルーティングテーブル（ユニキャストルーティング情報ベース（RIB）、静的 mroute など）から RPF 情報を検索できるため、**show ipv6 rpf** コマンドでは情報が取得される送信元を表示します。

Examples

次に、IPv6 アドレス 2001::1:1:2 を持つユニキャストホストの RPF 情報を表示する例を示します。

```
デバイス# show ipv6 rpf 2001::1:1:2
RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 92: show ipv6 rpf フィールドの説明

フィールド	説明
RPF information for 2001::1:1:2	この情報に関する送信元アドレス。
RPF interface:Ethernet3/2	指定した送信元について、ルータがパケットの取得を予定しているインターフェイス。
RPF neighbor:FE80::40:1:3	指定した送信元について、ルータがパケットの取得を予定しているネイバー。
RPF route/mask:20::/64	この送信元と照合するルート番号およびマスク。
RPF type:Unicast	このルートを取得したルーティングテーブル。ユニキャストまたは静的 mroute のいずれかです。
RPF recursion count	ルートが再帰的に解決された回数を示します。
Metric preference:110	代表フォワーダ (DF) によってアナウンされたルートプロセッサ (RP) に対してユニキャストルーティングメトリックを選択するために使用するプリフェレンス値。
Metric:30	DFによってアナウンされたRPに対するユニキャストルーティングメトリック。

show ipv6 source-guard policy

IPv6 送信元ガードポリシーの設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 source-guard policy** コマンドを使用します。

show ipv6 source-guard policy[*source-guard-policy*]

Syntax Description

<i>source-guard-policy</i>	スヌーピング ポリシーのユーザ定義名。ポリシー名には象徴的な文字列 (Engineering など) または整数 (0 など) を使用できます。
----------------------------	--

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 source-guard policy コマンドは、IPv6 送信元ガードポリシーの設定と、そのポリシーを適用するすべてのインターフェイスを表示します。また、このコマンドは、IPv6 プレフィックスガード機能がデバイス上で有効になっている場合は IPv6 プレフィックス ガード情報も表示します。

Examples

デバイス# **show ipv6 source-guard policy policy1**

```
Policy policy1 configuration:
data-glean
prefix-guard
address-guard
```

Policy policy1 is applied on the following targets:

Target	Type	Policy	Feature	Target range
Et0/0	PORT	policy1	source-guard	vlan all
vlan 100	VLAN	policy1	source-guard	vlan all

Related Commands

コマンド	説明
ipv6 source-guard attach-policy	インターフェイスに IPv6 ソースガードを適用します。
ipv6 source-guard policy	IPv6 送信元ガードポリシー名を定義して、送信元ガードポリシー設定モードを開始します。

show ipv6 spd

IPv6 選択的パケット破棄（SPD）設定を表示するには、特権 EXEC モードで **show ipv6 spd** コマンドを使用します。

show ipv6 spd

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines トラブルシューティングに役立つ情報が提供される場合がある SPD 設定を表示するには、**show ipv6 spd** コマンドを使用します。

Examples

次に、**show ipv6 spd** コマンドの出力例を示します。

```

デバイス# show ipv6 spd
Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 93: show ipv6 spd フィールドの説明

フィールド	説明
Current mode: normal	現在の SPD の状態またはモード。
Queue max threshold: 74	プロセス入力キューの最大値。

Related Commands

コマンド	説明
ipv6 spd queue max-threshold	SPD プロセス入力キュー内の最大パケット数を設定します。

show ipv6 static

IPv6 ルーティングテーブルの現在の内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 static** コマンドを使用します。

show ipv6 static [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface** *type number* | **recursive**] [**detail**]

Syntax Description	
<i>ipv6-address</i>	(任意) 特定の IPv6 アドレスのルーティング情報を提供します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>ipv6-prefix</i>	(任意) 特定の IPv6 ネットワークのルーティング情報を提供します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>/prefix-length</i>	(オプション) IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
interface	(任意) インターフェイスの名前。
<i>type</i>	(任意。ただし、 interface キーワードを使用した場合は必須) インターフェイスタイプ。サポートされているインターフェイスのタイプについては、疑問符 (?) のオンラインヘルプ機能を使用してください。
<i>number</i>	(任意。ただし、 interface キーワードを使用した場合は必須) インターフェイス番号。サポートされているインターフェイスの特定の番号シンタックスについては、疑問符 (?) のオンラインヘルプ機能を使用してください。
recursive	(任意) 再帰的な静的ルートのみを表示できます。
detail	(任意) 次の追加情報を指定します。 <ul style="list-style-type: none"> 有効な再帰ルートの場合は、出力パス セットおよび最大解決深度 無効な再帰ルートの場合は、ルートが有効でない理由 無効なダイレクトルートまたは完全指定のルートの場合は、ルートが有効でない理由

Command Default アクティブなすべてのルーティングテーブルのすべての IPv6 ルーティング情報が表示されます。

Command Modes ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ipv6 static コマンドは、IPv6 固有である点を除き、**show ip route** コマンドと同様の出力を提供します。

ipv6-address または *ipv6-prefix/prefix-length* 引数を指定すると、ルーティングテーブルから最長一致ルックアップが実行され、そのアドレスまたはネットワークのルート情報だけが表示されます。コマンド シンタックスで指定された条件に一致する情報だけが表示されます。たとえば、*type number* 引数を指定すると、指定したインターフェイス固有のルートのみが表示されます。

Examples

コマンド シンタックスでオプションが指定されていない **show ipv6 static** コマンド: 例

コマンドにオプションを使用しないと、IPv6 ルーティング情報ベース (RIB) にインストールされているルートがアスタリスクでマークされます。次に、この例を示します。

```
デバイス# show ipv6 static
```

```
IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 94: show ipv6 static フィールドの説明

フィールド	説明
via nexthop	リモートネットワークへのパス内にある次のデバイスのアドレスを指定します。
distance 1	指定したルートまでのアドミニストレーティブ ディスタンスを示します。

IPv6 アドレスとプレフィックスを指定した **show ipv6 static** コマンド: 例

ipv6-address 引数または *ipv6-prefix/prefix-length* 引数を指定すると、そのアドレスまたはネットワークの静的ルートに関する情報のみが表示されます。次に、IPv6 プレフィックス 2001:200::/35 を指定して入力した場合の **show ipv6 route** コマンドの出力例を示します。

```
デバイス# show ipv6 static 2001:200::/35
```

```
IPv6 Static routes
```

```
Code: * - installed in RIB
* 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
* 2001:200::/35, interface Ethernet2/0, distance 1
```

show ipv6 static interface コマンド: 例

インターフェイスを指定した場合、指定したインターフェイスを発信インターフェイスとして使用する静的ルートだけが表示されます。**interface** キーワードは、コマンドステートメント内に IPv6 アドレスとプレフィックスが指定されていても、されていなくても使用できます。

```
デバイス# show ipv6 static interface ethernet 3/0
```

```
IPv6 Static routes Code: * - installed in RIB 5000::/16, interface Ethernet3/0, distance 1
```

show ipv6 static recursive コマンド: 例

recursive キーワードを指定すると、再帰的な静的ルートのみが表示されます。

```
デバイス# show ipv6 static recursive
```

```
IPv6 Static routes Code: * - installed in RIB * 4000::/16, via nexthop 2001:1::1, distance 1 * 5555::/16,
via nexthop 4000::1, distance 1 5555::/16, via nexthop 9999::1, distance 1
```

show ipv6 static detail コマンド: 例

detail キーワードを指定した場合、次の追加情報が表示されます。

- 有効な再帰ルートの場合、出力パス セットおよび最大解決深度
- 無効な再帰ルートの場合、ルートが有効でない理由
- 無効なダイレクト ルートまたは完全指定のルートの場合、ルートが有効でない理由

```
デバイス# show ipv6 static detail
```

```
IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  Resolves to 1 paths (max depth 1)
  via Ethernet1/0
5000::/16, interface Ethernet3/0, distance 1
  Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
  Resolves to 1 paths (max depth 2)
  via Ethernet1/0
5555::/16, via nexthop 9999::1, distance 1
  Route does not fully resolve
```

show ipv6 static

```
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Related Commands

コマンド	説明
ipv6 route	静的 IPv6 ルートを確立します。
show ip route	ルーティング テーブルの現在の状態を表示します。
show ipv6 interface	IPv6 インターフェイス情報を表示します。
show ipv6 route summary	IPv6 ルーティング テーブルの現在の内容をサマリー形式で表示します。
show ipv6 tunnel	IPv6 トンネル情報を表示します。

show ipv6 traffic

IPv6 トラフィックを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 traffic** コマンドを使用します。

show ipv6 traffic [**interface**[*interface type number*]]

Syntax Description	interface	(任意) すべてのインターフェイス。IPv6 転送統計が保持されているすべてのインターフェイスの IPv6 転送統計が表示されます。
	<i>interface type number</i>	(任意) 指定したインターフェイス。特定のインターフェイス上で統計が最後にクリアされてから発生したインターフェイス統計が表示されます。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ipv6 traffic** コマンドは、IPv6 専用である点を除き、**show ip traffic** コマンドと同様の出力を提供します。

Examples

次に、**show ipv6 traffic** コマンドの出力例を示します。

```

デバイス# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a device
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd:  0 input, 0 checksum errors, 0 too short
         0 unknown info type, 0 unknown error type
  unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
         0 hopcount expired, 0 reassembly timeout, 0 too big
         0 echo request, 0 echo reply
         0 group query, 0 group report, 0 group reduce
         0 device solicit, 0 device advert, 0 redirects

```

次に、IPv6 CEF を実行しない **show ipv6 interface** コマンドの出力例を示します。

```

デバイス# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFE:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds

```

次に、IPv6 CEF を実行する **show ipv6 interface** コマンドの出力例を示します。

```

デバイス# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFE:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 95: show ipv6 traffic フィールドの説明

フィールド	説明
source-routed	送信元ルーティング パケットの数。
truncated	切り捨てられたパケットの数。
format errors	ヘッダー フィールド、バージョン番号、およびパケット長に実行したチェックにより発生した可能性のあるエラー。
not a device	IPv6 ユニキャスト ルーティングを有効にしていない場合に送信されるメッセージ。
0 unicast RPF drop, 0 suppressed RPF drop	ユニキャストと抑制されたリバース パス フォワーディング (RPF) のドロップの数
failed	失敗したフラグメント伝送の数。
encapsulation failed	未解決のアドレスまたは try-and-queue パケットにより発生する可能性のある障害。
no route	ルーティング方法が不明なデータグラムをソフトウェアが破棄するときにカウントされます。
unreach	受信した到達不能メッセージは次のとおりです。 <ul style="list-style-type: none"> • routing: 宛先までのルートがないことを示します。 • admin: 宛先との通信が管理上の理由で禁止されていることを示します。 • neighbor: 宛先が送信元アドレスの範囲を超えていることを示します。たとえば、送信元がローカル サイトであるか、または送信元に戻るルートが宛先にない場合があります。 • address: アドレスに到達不能であることを示します。 • port: ポートに到達不能であることを示します。
Unicast RPF access-list MINI	使用中のユニキャスト RPF アクセスリスト。
Process Switching	検証ドロップや抑制された検証ドロップなどのプロセス RPF カウントを表示します。
CEF Switching	検証ドロップや抑制された検証ドロップなどの CEF スイッチング カウントを表示します。

show key chain

キーチェーンを表示するには、**show key chain** コマンドを使用します。

show key chain [*name-of-chain*]

Syntax Description

<i>name-of-chain</i>	(任意) キーチェーンコマンドで命名された表示対象のキーチェーン名。
----------------------	------------------------------------

Command Default

パラメータを指定せずにコマンドを使用すると、すべてのキーチェーンのリストを表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**show key chain** コマンドの出力例を示します。

```

show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
  key 1 -- text "Thisisasecretkey"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
  key 100 -- text "abc123"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]

```

Related Commands

コマンド	説明
key-string	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。

show track

トラッキングプロセスが追跡したオブジェクトに関する情報を表示するには、特権 EXEC モードで **show track** コマンドを使用します。

show track [*object-number* [brief] | **application** [brief] | **interface** [brief] | **ip**[route [brief] | [sla [brief]] | **ipv6** [route [brief]] | **list** [route [brief]] | **resolution** [ip | ipv6] | **stub-object** [brief] | **summary** | **timers**]

Syntax Description

<i>object-number</i>	(任意) トラッキング対象オブジェクトを表すオブジェクト番号。範囲は 1 ~ 1000 です。
brief	(任意) 先行する引数やキーワードに関連する 1 行の情報を表示します。
application	(任意) トラッキング対象のアプリケーション オブジェクトを表示します。
interface	(任意) トラッキング対象のインターフェイス オブジェクトを表示します。
ip route	(任意) トラッキング対象の IP ルート オブジェクトを表示します。
ip sla	(任意) トラッキング対象の IP SLA オブジェクトを表示します。
ipv6 route	(任意) トラッキング対象の IPv6 ルート オブジェクトを表示します。
list	(任意) プール オブジェクトを表示します。
resolution	(任意) トラッキング対象パラメータの解像度を表示します。
summary	(任意) 指定されたオブジェクトの概要を表示します。
timers	(任意) ポーリング間隔タイマーを表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

トラッキングプロセスによってトラッキングされているオブジェクトに関する情報を表示するには、このコマンドを使用します。引数やキーワードを指定しない場合は、すべてのオブジェクトの情報が表示されます。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうか

は、使用可能なCPUによって異なります。特定のサイトトラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

Examples

次に、インターフェイスで IP ルーティングの状態をトラッキングした場合の例を示します。

```
Device# show track 1

Track 1
  Interface GigabitEthernet 1/0/1 ip routing
  IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 96: show track フィールドの説明

フィールド	説明
Track	トラッキング対象オブジェクトの数。
Interface GigabitEthernet 1/0/1 IP routing	インターフェイスタイプ、インターフェイス番号、およびトラッキング対象オブジェクト。
IP routing is	Up または Down で表示されるオブジェクトの状態の値。オブジェクトがダウンしている場合は、理由が示されます。
1 change、last change	トラッキング対象オブジェクトの状態が変更された回数と、最後の変更からの経過時間（hh:mm:ss で表示）。

Related Commands

Command	Description
show track resolution	追跡対象パラメータの解像度を表示します。
track interface	インターフェイスをトラッキングされるように設定し、トラッキングコンフィギュレーションモードを開始します。
track ip route	IP ルートの状態を追跡し、トラッキングコンフィギュレーションモードを開始します。

track

Gateway Load Balancing Protocol (GLBP) の重み付けがインターフェイスの状態に基づいて変更されている場合にトラッキング対象インターフェイスを設定するには、グローバル コンフィギュレーションモードで **track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

```
track object-number interface type number {line-protocol|ip routing | ipv6 routing}
no track object-number interface type number {line-protocol|ip routing | ipv6 routing}
```

Syntax Description

<i>object-number</i>	トラッキングされるインターフェイスを表すオブジェクト番号。値の範囲は 1 ~ 1000 です。
interface <i>type number</i>	トラッキングするインターフェイス タイプおよび番号。
line-protocol	インターフェイスがアップ状態かどうかをトラッキングします。
ip routing	インターフェイスがアップの状態であることを GLBP に報告する前に、IP ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。
ipv6 routing	インターフェイスがアップの状態であることを GLBP に報告する前に、IPv6 ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。

Command Default

インターフェイスの状態はトラッキングされません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

トラッキング対象インターフェイスのパラメータを設定するには、**track** コマンドと併せて **glbp weighting** および **glbp weighting track** コマンドを使用します。GLBP デバイスのトラッキング対象インターフェイスがダウンすると、そのデバイスの重み値は減らされます。重み値が指定された最小値を下回った場合、デバイスは、アクティブ GLBP 仮想フォワーダとしての機能を失います。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうか

は、使用可能なCPUによって異なります。特定のサイトトラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

Examples

次に、TenGigabitEthernet インターフェイス 0/0/1 が、GigabitEthernet インターフェイス 1/0/1 および 1/0/3 がアップの状態にあるかどうかをトラッキングする例を示します。GigabitEthernet インターフェイスのいずれかがダウンすると、GLBP の重み値は、デフォルト値である 10 まで減らされます。両方の GigabitEthernet インターフェイスがダウンすると、GLBP の重み値は下限しきい値未満に下がり、デバイスはアクティブフォワーダではなくなります。アクティブフォワーダとしての役割を再開するには、デバイスは、両方のトラッキング対象インターフェイスをアップの状態に戻し、重み値を上限しきい値を超える値に上げる必要があります。

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

Related Commands

コマンド	説明
glbp weighting	GLBP ゲートウェイの初期重み値を指定します。
glbp weighting track	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。

vrrp

Virtual Router Redundancy Protocol バージョン 3 (VRRPv3) グループを作成し、VRRPv3 グループ コンフィギュレーションモードを開始するには、**vrrp** を使用します。VRRPv3 グループを削除するには、このコマンドの **no** 形式を使用します。

```
vrrp group-id address-family {ipv4 | ipv6}
no vrrp group-id address-family {ipv4 | ipv6}
```

Syntax Description

group-id	仮想ルータ グループ番号。範囲は 1 ~ 255 です。
address-family	この VRRP グループのアドレス ファミリを指定します。
ipv4	(任意) IPv4 アドレスを指定します。
ipv6	(任意) IPv6 アドレスを指定します。

Command Default

なし

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Examples

次の例は、VRRPv3 グループの作成方法と VRRP コンフィギュレーション モードの開始方法を示しています。

```
Device(config-if)# vrrp 3 address-family ipv4
```

Related Commands

コマンド	説明
timers advertise	アドバタイズメントタイマーを設定します (ミリ秒単位)。

vrrp description

Virtual Router Redundancy Protocol (VRRP) に説明を割り当てるには、インターフェイス コンフィギュレーション モードで **vrrp description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *text*

no description

Syntax Description

<i>text</i>	グループの目的または用途を説明するテキスト（最大 80 文字）。
-------------	----------------------------------

Command Default

VRRP グループの説明はありません。

Command Modes

VRRP 設定 (config-if-vrrp)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の例では、VRRP を有効にしています。VRRP グループ 1 は、「Building A – Marketing and Administration (ビルディング A: マーケティングおよび管理)」と説明されます。

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

Related Commands

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。

vrrp preempt

デバイスに現在のプライマリ仮想ルータより高い優先順位が与えられている場合、そのデバイスが Virtual Router Redundancy Protocol (VRRP) グループのプライマリ仮想ルータの機能を引き継ぐように設定するには、VRRP コンフィギュレーションモードで **preempt** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

preempt [**delay minimum seconds**]
no preempt

Syntax Description	delay minimum seconds	(任意) プライマリの所有権を要求するアドバタイズメントを発行するまでに、デバイスが待機する秒数。デフォルト遅延値は 0 秒です。
---------------------------	------------------------------	---

Command Default このコマンドは有効です。

Command Modes VRRP 設定 (config-if-vrrp)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デフォルトでは、このコマンドで設定されるデバイスは、現在のプライマリ仮想ルータよりも高い優先順位を持つ場合、プライマリ仮想ルータとしての機能を引き継ぎます。VRRP デバイスが、プライマリ所有権を要求するアドバタイズメントを発行するまで、指定された秒数待機するように遅延時間を設定できます。



Note このコマンドの設定にかかわらず、IP アドレスの所有者であるデバイスがプリエンプション処理します。

Examples

次に、デバイスの 200 の優先順位が現在のプライマリ仮想ルータの優先順位よりも高い場合に、デバイスが現在のプライマリ仮想ルータをプリエンプション処理するように設定する例を示します。デバイスは、現在のプライマリ仮想ルータをプリエンプション処理する場合、プライマリ仮想ルータであることを要求するアドバタイズメントを発行するまでに 15 秒待機します。

```
Device(config-if-vrrp)#preempt delay minimum 15
```

Related Commands

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
priority	VRRP グループ内のデバイスの優先度レベルを設定します。

vrrp priority

Virtual Router Redundancy Protocol (VRRP) 内のデバイスの優先度レベルを設定するには、インターフェイス コンフィギュレーション モードで **priority** コマンドを使用します。デバイスの優先度レベルを削除するには、このコマンドの **no** 形式を使用します。

priority *level*

no priority *level*

Syntax Description	<i>level</i>	VRRP グループ内のデバイスの優先順位。有効な範囲は 1 ~ 254 です。デフォルトは 100 です。
---------------------------	--------------	---

Command Default 優先度レベルはデフォルト値の 100 に設定されています。

Command Modes VRRP 設定 (config-if-vrrp)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドを使用すると、どのデバイスをプライマリ仮想ルータにするかを制御できます。

Examples

次に、デバイスを 254 の優先順位に設定する例を示します。

```
Device(config-if-vrrp)# priority 254
```

Related Commands	コマンド	説明
	vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
	vrrp preempt	デバイスに現在のプライマリ仮想ルータより高い優先順位が与えられている場合、そのデバイスが VRRP グループのプライマリ仮想ルータの機能を引き継ぐように設定します。

vrrp timers advertise

Virtual Router Redundancy Protocol (VRRP) グループ内のプライマリ仮想ルータによる連続したアドバタイズメント間の間隔を設定するには、VRRP コンフィギュレーション モードで **timers advertise** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers advertise [msec] interval
no timers advertise [msec] interval

Syntax Description

<i>group</i>	仮想ルータ グループ番号。グループ番号の範囲は 1 ～ 255 です。
<i>msec</i>	(任意) アドバタイズメント時間の単位を秒からミリ秒に変更します。このキーワードを付加しないと、アドバタイズメント間隔は秒単位になります。
<i>interval</i>	プライマリ仮想ルータによる連続したアドバタイズメント間の時間間隔。 msec キーワードを指定しなかった場合、間隔は秒単位になります。デフォルト値は 1 秒です。有効範囲は 1 ～ 255 秒です。 msec キーワードを指定した場合、有効な範囲は 50 ～ 999 ミリ秒です。

Command Default

デフォルトの間隔である 1 秒に設定されています。

Command Modes

VRRP 設定 (config-if-vrrp)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

プライマリ仮想ルータから送信されるアドバタイズメントは、現在のプライマリ仮想ルータの状態と優先順位を伝えます。

vrrp timers advertise コマンドは、連続するアドバタイズメントパケットの間の時間間隔と、プライマリルータがダウンしていると他のルータが宣言するまでの時間を設定します。タイマー値が設定されていないルータまたはアクセスサーバは、プライマリルータからタイマー値を取得できません。プライマリルータで設定されたタイマーは、他のすべてのタイマー設定を常に上書きします。VRRP グループ内のすべてのルータが同じタイマー値を使用する必要があります。同じタイマー値が設定されていないと、VRRP グループ内のデバイスが相互通信せず、正しく設定されていないデバイスのステータスがプライマリに変わります。

Examples

次に、プライマリ仮想ルータがアドバタイズメントを 4 秒ごとに送信するように設定する例を示します。

```
Device(config-if-vrrp)# timers advertise 4
```

Related Commands

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
timers learn	VRRP グループのバックアップ仮想ルータとして動作するときに、プライマリ仮想ルータが使用していたアドバタイズ間隔を学習するようにデバイスを設定します。

vrrs leader

リーダーの名前を Virtual Router Redundancy Service (VRRS) に登録されるように指定するには、**vrrs leader** コマンドを使用します。指定された VRRS リーダーを削除するには、このコマンドの **no** 形式を使用します。

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

Syntax Description

<i>vrrs-leader-name</i>	リードする VRRS タグの名前。
-------------------------	-------------------

Command Default

登録済みの VRRS 名はデフォルトで使用不可になっています。

Command Modes

VRRP 設定 (config-if-vrrp)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、VRRS に登録されるリーダーの名前を指定する例を示します。

```
Device(config-if-vrrp)# vrrs leader leader-1
```

Related Commands

コマンド	説明
vrrp	VRRP グループを作成し、VRRP コンフィギュレーションモードを開始します。



PART **V**

IP マルチキャスト ルーティング

- [IP マルチキャスト ルーティング コマンド, on page 725](#)



IP マルチキャスト ルーティング コマンド

- [clear ip mfib counters, on page 727](#)
- [clear ip mroute, on page 728](#)
- [clear ip pim snooping vlan, on page 730](#)
- [debug condition vrf, on page 731](#)
- [debug ip pim, on page 733](#)
- [debug ipv6 pim, on page 735](#)
- [ip igmp filter, on page 738](#)
- [ip igmp max-groups, on page 739](#)
- [ip igmp profile, on page 741](#)
- [ip igmp snooping, on page 743](#)
- [ip igmp snooping last-member-query-count, on page 744](#)
- [ip igmp snooping querier, on page 746](#)
- [ip igmp snooping report-suppression, on page 749](#)
- [ip igmp snooping vlan mrouter, on page 750](#)
- [ip igmp snooping vlan static, on page 751](#)
- [ip multicast auto-enable, on page 753](#)
- [ip multicast-routing, on page 754](#)
- [ip pim accept-register, on page 755](#)
- [ip pim bsr-candidate, on page 757](#)
- [ip pim rp-candidate, on page 759](#)
- [ip pim send-rp-announce, on page 761](#)
- [ip pim snooping, on page 763](#)
- [ip pim snooping dr-flood, on page 764](#)
- [ip pim snooping vlan, on page 765](#)
- [ip pim spt-threshold, on page 766](#)
- [match message-type, on page 767](#)
- [match service-type, on page 768](#)
- [match service-instance, on page 769](#)
- [mrinfo, on page 770](#)
- [service-policy-query, on page 772](#)
- [service-policy, on page 773](#)
- [show ip igmp filter, on page 774](#)
- [show ip igmp profile, on page 775](#)

- [show ip igmp snooping](#), on page 776
- [show ip igmp snooping groups](#), on page 778
- [show ip igmp snooping mrouter](#), on page 779
- [show ip igmp snooping querier](#), on page 780
- [show ip pim autorp](#), on page 782
- [show ip pim bsr-router](#), on page 783
- [show ip pim bsr](#), on page 784
- [show ip pim snooping](#), on page 785
- [show ip pim tunnel](#), on page 788
- [show platform software fed switch ip multicast](#), on page 790

clear ip mfib counters

すべてのアクティブ IPv4 マルチキャスト転送情報ベース (MFIB) トラフィックカウンタをクリアするには、特権 EXEC モードで **clear ip mfib counters** コマンドを使用します。

clear ip mfib [**global** | **vrf ***] **counters** [*group-address*] [*hostname* | *source-address*]

Syntax Description	global	(任意) IP MFIB キャッシュをグローバルデフォルト設定にリセットします。
	vrf *	(任意) すべての VPN ルーティングおよび転送インスタンスの IP MFIB キャッシュをクリアします。
	<i>group-address</i>	(任意) アクティブ MFIB トラフィックカウンタを指定されたグループアドレスに制限します。
	<i>hostname</i>	(任意) アクティブ MFIB トラフィックカウンタを指定されたホスト名に制限します。
	<i>source-address</i>	(任意) アクティブ MFIB トラフィックカウンタを指定された送信元アドレスに制限します。
Command Default	なし	
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、すべてのマルチキャストテーブルのアクティブ MFIB トラフィックカウンタをすべてリセットする例を示します。

```
デバイス# clear ip mfib counters
```

次に、IP MFIB キャッシュカウンタをグローバルデフォルト設定にリセットする例を示します。

```
デバイス# clear ip mfib global counters
```

次に、すべての VPN ルーティングおよび転送インスタンスの IP MFIB キャッシュをクリアする例を示します。

```
デバイス# clear ip mfib vrf * counters
```

clear ip mroute

IP マルチキャストルーティング テーブルのエントリを削除するには、特権 EXEC モードで **clear ip mroute** コマンドを使用します。

```
clear ip mroute [vrf vrf-name] [* | ip-address | group-address] [hostname | source-address]
```

Syntax Description	
vrf <i>vrf-name</i>	(任意) マルチキャスト VPN ルーティング/転送 (VRF) インスタンスに割り当てられている名前を指定します。
*	すべてのマルチキャストルート指定します。
<i>ip-address</i>	IP アドレスのマルチキャストルート。
<i>group-address</i>	グループアドレスのマルチキャストルート。
<i>hostname</i>	(任意) ホスト名のマルチキャストルート。
<i>source-address</i>	(任意) 送信元アドレスのマルチキャストルート。

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines *group-address* 変数は、次のいずれかを指定します。

- DNS ホストテーブルまたは **ip host** コマンドで定義されるマルチキャストグループ名
- 4 分割ドット表記によるマルチキャストグループの IP アドレス

group の名前またはアドレスを指定する場合、*source* 引数を入力して、グループに送信するマルチキャスト送信元の名前またはアドレスも指定できます。送信元は、グループのメンバである必要はありません。

例

次に、IP マルチキャストルーティング テーブルからすべてのエントリを削除する例を示します。

```
デバイス# clear ip mroute *
```

次に、マルチキャストグループ 224.2.205.42 に送信する 228.3.0.0 サブネット上のすべての送信元を IP マルチキャストルーティングテーブルから削除する例を示します。この例では、ネットワーク 228.3 上の個別の送信元ではなく、すべての送信元が削除されます。

```
デバイス# clear ip mroute 224.2.205.42 228.3.0.0
```

clear ip pim snooping vlan

特定の VLAN 上の Protocol Independent Multicast (PIM) スヌーピングエントリを削除するには、ユーザ EXEC または特権 EXEC モードで **clear ip pim snooping vlan** コマンドを使用します。

clear ip pim snooping vlan *vlan-id* [**neighbor** | **statistics** | **mroute** [*source-ipgroup-ip*]]

Syntax Description		
vlan <i>vlan-id</i>		VLAN ID。有効な値の範囲は 1 ~ 4094 です。
neighbor		すべてのネイバーを削除します。
statistics		VLAN 統計の情報を削除します。
mroute <i>group-addr src-addr</i>		指定したグループおよび送信元 IP アドレスの mroute エントリを削除します。

Command Default このコマンドには、デフォルト設定がありません。

Command Modes ユーザ EXEC
特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples 次に、特定の VLAN 上の IP PIM スヌーピングエントリをクリアする例を示します。

```
Router# clear ip pim snooping vlan 1001
```

Related Commands	コマンド	説明
	ip pim snooping	PIM スヌーピングをグローバルにイネーブルにします。
	show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

debug condition vrf

デバッグ出力を特定の仮想ルーティングおよび転送（VRF）インスタンスに制限するには、特権 EXEC モードで **debug condition vrf** コマンドを使用します。条件を削除するには、このコマンドの **no** 形式を使用します。

```
debug condition vrf {default | global | green | name {vrf-name | green}}
```

```
no debug condition vrf {default | global | green | name {vrf-name | green}}
```

構文の説明

構文	説明
default	デフォルトのルーティングテーブルを指定します。
global	グローバルルーティングテーブルを指定します。
green	VRF 名を指定します。
name <i>vrf-name</i>	ルーティングテーブルの名前を指定します。

Command Modes

特権 EXEC モード (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを使用して、デバッグ出力を単一の VRF に制限します。



Caution

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワークトラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性があります。

例

次に、VRF red にデバッグ出力を制限する例を示します。

```
Device# debug condition vrf red
```

debug ip pim

送受信された PIM パケット、および PIM 関連のイベントを表示するには、特権 EXEC モードで **debug ip pim** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug ip pim [vrf vrf-name ][ip-address | atm | auto-rp | bfd | bsr | crimson | df rp-address | drlb | hello | timers]
```

```
no debug ip pim [vrf vrf-name ][ip-address | atm | auto-rp | bfd | bsr | crimson | df rp-address | drlb | hello | timers]
```

構文の説明

構文	説明
vrf <i>vrf-name</i>	(任意) VPN ルーティングおよび転送インスタンスを指定します。 このキーワードは、 debug condition vrf vrf-name コマンドで指定された VRF のデバッグを上書きします。
<i>ip-address</i>	(任意) IP グループアドレスを指定します。
atm	(任意) PIM ATM シグナリングアクティビティに関するデバッグ情報を表示します。
auto-rp	(任意) Auto-RP 情報のデバッグ情報を表示します。
bfd	(任意) BFD コンフィギュレーションのデバッグ情報を表示します。
bsr	(任意) PIM Candidate-RP および BSR アクティビティに関するデバッグ情報を表示します。
crimson	(任意) Crimson データベースアクティビティに関するデバッグ情報を表示します。
df <i>rp-address</i>	(任意) PIM RP 指定フォワーダ選択アクティビティに関するデバッグ情報を表示します。
drlb	(任意) PIM 指定ルータのロードバランシングアクティビティに関するデバッグ情報を表示します。

構文	説明
hello	(任意) 送受信された PIM Hello パケットに関するデバッグ情報を表示します。
timers	(任意) PIM タイマーイベントに関するデバッグ情報を表示します。

Command Modes 特権 EXEC モード (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Caution デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワークトラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

PIM で一度に最大 8 つの VRF をデバッグできます。複数の VRF を同時にデバッグするには、次の一連の手順を実行します。

```
debug condition vrf vrf-name1
debug condition vrf vrf-name2
.
.
.
debug condition vrf vrf-name8
debug ip pim
```

例

次に、Crimson データベースアクティビティを表示する例を示します。

```
Device# debug ip pim crimson
```

次に、PIM の 2 つの VRF red と green を同時にデバッグする例を示します。

```
Device# debug condition vrf red
Device# debug condition vrf green
Device# debug ip pim
```

debug ipv6 pim

Protocol Independent Multicast (PIM) プロトコルアクティビティのデバッグを有効にするには、特権 EXEC モードで **debug ipv6 pim** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
debug ipv6 pim
[vrf vrf-name ]
[bfd interface-type interface-number | bsr | crimson | df-election [interface interface-type
interface-number | rp rp-address] | drlb | group group-address | interface interface-type
interface-number | limit [group-address] | neighbor interface-type interface-number ]
```

```
no debug ipv6 pim
[vrf vrf-name ]
[bfd interface-type interface-number | bsr | crimson | df-election [interface interface-type
interface-number | rp rp-address] | drlb | group group-address | interface interface-type
interface-number | limit [group-address] | neighbor interface-type interface-number ]
```

構文の説明

構文	説明
vrf vrf-name	(任意) VPN ルーティングおよび転送インスタンスを指定します。 このキーワードは、 debug condition vrf vrf-name コマンドで指定された VRF のデバッグを上書きします。
bfd	(任意) BFD コンフィギュレーションのデバッグ情報を表示します。
bsr	(任意) 送受信された PIM Candidate-RP および BSR に関するデバッグ情報を表示します。
crimson	(任意) Crimson データベースアクティビティに関するデバッグ情報を表示します。
df-election	(任意) PIM 指定フォワード選択アクティビティに関するデバッグ情報を表示します。
drlb	(任意) PIM 指定ルータのロードバランシングアクティビティに関するデバッグ情報を表示します。
group group-address	(任意) グループ関連アクティビティに関するデバッグ情報を表示します。

構文	説明
interface	(任意) 指定されたインターフェイスのプロトコルアクティビティに関するデバッグ情報を表示します。
limit	(任意) インターフェイス制限に関するデバッグ情報を表示します。
neighbor	(任意) 送受信された PIM Hello メッセージに関するデバッグ情報を表示します。
<i>interface-type interface-number</i>	(任意) 指定されたインターフェイスに関するデバッグ情報を表示します。
rp rp-address	(任意) 指定された RP に関するデバッグ情報を表示します。

Command Modes

特権 EXEC モード (#)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines**Caution**

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワークトラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

PIM で一度に最大 8 つの VRF をデバッグできます。複数の VRF を同時にデバッグするには、次の一連の手順を実行します。

```
debug condition vrf vrf-name1
debug condition vrf vrf-name2
.
.
.
debug condition vrf vrf-name8
debug ip pim
```

例

次に、Crimson データベースアクティビティを表示する例を示します。

```
Device# debug ipv6 pim crimson
```

次に、VRF red をデバッグする例を示します。

```
Device# debug vrf red ipv6 pim
```

ip igmp filter

Internet Group Management Protocol (IGMP) プロファイルをインターフェイスに適用することで、レイヤ2 インターフェイスのすべてのホストが1つ以上の IP マルチキャストグループに参加できるかどうかを制御するには、**device** スタックまたはスタンドアロン **device** で **ip igmp filter** インターフェイスコンフィギュレーションコマンドを使用します。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*
no ip igmp filter

Syntax Description	<i>profile number</i> 適用する IGMP プロファイル番号。範囲は1～4294967295です。				
Command Default	IGMP フィルタは適用されていません。				
Command Modes	インターフェイス コンフィギュレーション (config-if)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	<p>IGMP フィルタはレイヤ2の物理インターフェイスだけに適用できます。ルーテッドポート、Switch Virtual Interface (SVI)、または EtherChannel グループに属するポートに対して IGMP フィルタを適用することはできません。</p> <p>IGMP プロファイルは1つまたは複数の device ポートインターフェイスに適用できますが、1つのポートに対して1つのプロファイルだけ適用できます。</p> <p>例</p> <p>設定を確認するには、特権 EXEC モードで show running-config コマンドを使用してインターフェイスを指定します。</p>				

ip igmp max-groups

レイヤ 2 インターフェイスが参加可能な Internet Group Management Protocol (IGMP) グループの最大数を設定するか、最大数のエントリが転送テーブルにあるときの IGMP スロットリングアクションを設定するには、**device** スタックまたはスタンドアロン **device** で **ip igmp max-groups** インターフェイスコンフィギュレーションコマンドを使用します。最大数をデフォルト値（無制限）に戻すか、デフォルトのスロットリングアクション（レポートをドロップ）に戻すには、このコマンドの **no** 形式を使用します。

```
ip igmp max-groups {max number | action { deny | replace }}
no ip igmp max-groups {max number | action }
```

Syntax Description

<i>max number</i>	インターフェイスが参加できる IGMP グループの最大数。範囲は 0～4294967294 です。デフォルト設定は無制限です。
action deny	最大数のエントリが IGMP スヌーピング転送テーブルにある場合は、次の IGMP 参加レポートをドロップします。これがデフォルトのアクションになります。
action replace	最大数のエントリが IGMP スヌーピング転送テーブルにある場合に、IGMP レポートを受信した既存のグループを新しいグループで置き換えます。

Command Default

デフォルトの最大グループ数は制限なしです。

インターフェイス上に IGMP グループエントリの最大数があることを **device** が学習した後の、デフォルトのスロットリングアクションでは、インターフェイスが受信する次の IGMP レポートをドロップし、インターフェイスに IGMP グループのエントリを追加しません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、レイヤ 2 物理インターフェイスおよび論理 EtherChannel インターフェイスでだけ使用できます。ルーテッドポート、Switch Virtual Interface (SVI)、または EtherChannel グループに属するポートに対して IGMP 最大グループ数を設定することはできません。

IGMP スロットリングアクションを設定する場合には、次の注意事項に従ってください。

- スロットリングアクションを **deny** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れた後で、エントリの最大数が転送テーブルにある場合は、インターフェイス上で受信された次の IGMP レポートを **device** がドロップします。
- スロットリングアクションを **replace** として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは削除されます。最大数のエントリが転送テーブルにある場

合、**device**はランダムに選択したマルチキャストエントリを受信したIGMPレポートで置き換えます。

- グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups {deny | replace}** コマンドを入力しても効果はありません。

例

次に、ポートが加入できるIGMPグループ数を25に制限する例を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
```

```
デバイス(config-if)# ip igmp max-groups 25
```

次に、最大数のエントリが転送テーブルにあるときに、IGMPレポートを受信した既存のグループを新しいグループと置き換えるように**device**を設定する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
```

```
デバイス(config-if)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

ip igmp profile

Internet Group Management Protocol (IGMP) プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始するには、`device` スタックまたはスタンドアロン `device` で `ip igmp profile` グローバルコンフィギュレーション コマンドを使用します。このモードで、スイッチポートからの IGMP メンバーシップレポートをフィルタリングするための IGMP プロファイルの設定を指定できます。IGMP プロファイルを削除するには、このコマンドの `no` 形式を使用します。

```
ip igmp profile profile number
no ip igmp profile profile number
```

Syntax Description	<code>profile number</code> 設定する IGMP プロファイル番号。範囲は 1～4294967295 です。				
Command Default	IGMP プロファイルは定義されていません。設定された場合、デフォルトの IGMP プロファイルとの一致機能は、一致するアドレスを拒否する設定になります。				
Command Modes	グローバル コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	<p>IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。</p> <ul style="list-style-type: none"> • deny: 一致するアドレスを拒否するように指定します (デフォルト設定の状態)。 • exit: IGMP プロファイル コンフィギュレーション モードを終了します。 • no: コマンドを無効にする、またはデフォルトにリセットします。 • permit: 一致するアドレスを許可するように指定します。 • range: プロファイルの IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。 <p>範囲を入力する場合、低い方の IP マルチキャストアドレスを入力してからスペースを入力し、次に高い方の IP マルチキャストアドレスを入力します。</p> <p>IGMP のプロファイルを、1 つまたは複数のレイヤ 2 インターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つだけです。</p>				

例

次の例では、指定された範囲の IP マルチキャストアドレスを許可する IGMP プロファイル 40 の設定方法を示します。

```
デバイス(config)# ip igmp profile 40
デバイス(config-igmp-profile)# permit
デバイス(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

設定を確認するには、特権 EXEC モードで **show ip igmp profile** コマンドを使用します。

ip igmp snooping

device で Internet Group Management Protocol (IGMP; インターネットグループ管理プロトコル) スヌーピングをグローバルにイネーブルにするか、または VLAN 単位でイネーブルにするには、device スタックまたはスタンドアロン device で **ip igmp snooping** グローバルコンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id* (任意) 指定された VLAN で IGMP スヌーピングをイネーブルにします。範囲は 1 ~ 1001 および 1006 ~ 4094 です。

Command Default

device 上で、IGMP スヌーピングはグローバルに有効になっています。
VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip igmp snooping last-member-query-count

Internet Group Management Protocol (IGMP) スヌーピングが IGMP 脱退メッセージの受信に対してクエリーメッセージを送信する回数を設定するには、グローバルコンフィギュレーションモードで **ip igmp snooping last-member-query-count** コマンドを使用します。count をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

```
ip igmp snooping [vlan vlan-id] last-member-query-count count
no ip igmp snooping [vlan vlan-id] last-member-query-count count
```

Syntax Description	vlan vlan-id (任意) 特定の VLAN ID のカウント値を指定します。範囲は 1 ~ 1001 です。先頭の 0 は入力しないでください。				
	count クエリーメッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1 ~ 7 です。デフォルトは 2 です。				
Command Default	クエリーが 2 ミリ秒ごとに送信されます。				
Command Modes	グローバル コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines マルチキャストホストがグループから脱退すると、ホストは IGMP 脱退メッセージを送信します。このホストがグループを脱退する最終ホストかどうかを確認するために、脱退メッセージが確認されると、**last-member-query-interval** タイムアウト期間が過ぎるまで IGMP クエリーメッセージが送信されます。タイムアウト期限が切れる前に last-member クエリーへの応答が受信されないと、グループレコードは削除されます。

タイムアウト期間を設定するには、**ip igmp snooping last-member-query-interval** コマンドを使用します。

IGMP スヌーピング即時脱退処理とクエリーカウントの両方を設定した場合は、即時脱退処理が優先されます。



Note カウントを 1 に設定しないでください。単一パケットの損失 (device からホストへのクエリーパケット、またはホストから device へのレポートパケット) により、受信者がまだいてもトラフィックの転送が停止される場合があります。トラフィックは、次の一般クエリーが device から送信された後も転送され続けますが、受信者がクエリーを受信しない間隔は 1 分間 (デフォルトのクエリー間隔) となる可能性があります。

Cisco IOS ソフトウェアの脱退遅延は、device が last-member-query-interval (LMQI) 内で複数の脱退を処理しているときに、1 つの LMQI 値まで増やすことができます。このシナリオでは、平均脱退遅延は (カウント数 + 0.5) * LMQI によって決まります。その結果、デフォルトの脱退遅延は 2.0 ~ 3.0 秒の範囲となり、IGMP 脱退処理の負荷が高い状態では平均 2.5 秒となります。100 ミリ秒でカウントが 1 という LMQI の最小値の負荷条件下では、脱退遅延は 100 ~ 200 ミリ秒となり、平均は 150 ミリ秒です。これは、高レート of IGMP 脱退メッセージから受ける影響を抑えるために行われます。

例

次に、最後のメンバクエリーの数を 5 に設定する例を示します。

```
デバイス(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

レイヤ 2 ネットワークで Internet Group Management Protocol (IGMP) クエリア機能をグローバルにイネーブルにするには、**ip igmp snooping querier** グローバルコンフィギュレーションコマンドを使用します。キーワードとともにコマンドを入力すると、VLAN インターフェイスの IGMP クエリア機能をイネーブルにし、設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]

no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** | **version**]

Syntax Description

vlan <i>vlan-id</i>	(任意) 指定された VLAN で IGMP スヌーピングおよび IGMP クエリア機能をイネーブルにします。範囲は 1 ~ 1001 および 1006 ~ 4094 です。
address <i>ip-address</i>	(任意) 送信元 IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。
max-response-time <i>response-time</i>	(任意) IGMP クエリアレポートを待機する最長時間を設定します。範囲は 1 ~ 25 秒です。
query-interval <i>interval-count</i>	(任意) IGMP クエリアの間隔を設定します。範囲は 1 ~ 18000 秒です。
tcn query	(任意) トポロジ変更通知 (TCN) に関連するパラメータを設定します。
count <i>count</i>	TCN 時間間隔に実行される TCN クエリの数を設定します。範囲は 1 ~ 10 です。
interval 間隔	TCN クエリの時間間隔を設定します。範囲は 1 ~ 255 です。
timer expiry <i>expiry-time</i>	(任意) IGMP クエリアが期限切れになる時間を設定します。範囲は 60 ~ 300 秒です。
version <i>version</i>	(任意) クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。

Command Default

IGMP スヌーピングクエリア機能は、**device** でグローバルにディセーブルに設定されています。

IGMP スヌーピングクエリアは、イネーブルの場合でも、マルチキャストルータからの IGMP トラフィックが検出されると、自らをディセーブルにします。

Command Modes	グローバル コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines クエリアとも呼ばれる IGMP クエリメッセージを送信するデバイスの IGMP バージョンおよび IP アドレスを検出するために IGMP スヌーピングをイネーブルにするには、このコマンドを使用します。

デフォルトでは、IGMP スヌーピングクエリアは、IGMP バージョン 2 (IGMPv2) を使用するデバイスを検出するように設定されていますが、IGMP バージョン 1 (IGMPv1) を使用しているクライアントは検出しません。デバイスが IGMPv2 を使用している場合、**max-response-time** 値を手動で設定できます。デバイスが IGMPv1 を使用している場合は、max-response-time を設定できません (値を設定できず、0 に設定されています)。

IGMPv1 を実行している RFC に準拠していないデバイスは、**max-response-time** 値としてゼロ以外の値を持つ IGMP 一般クエリメッセージを拒否することがあります。デバイスで IGMP 一般クエリメッセージを受け入れる場合、IGMP スヌーピングクエリアが IGMPv1 を実行するように設定します。

VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングクエリア機能をグローバルにイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping querier
```

次の例では、IGMP スヌーピングクエリアの最大応答時間を 25 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピングクエリアの時間間隔を 60 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier query-interval 60
```

次の例では、IGMP スヌーピングクエリアの TCN クエリカウントを 25 に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier tcn count 25
```

次の例では、IGMP スヌーピングクエリアのタイムアウト値を 60 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier timer expiry 60
```

次に、IGMP スヌーピングクエリア機能をバージョン 2 に設定する例を示します。

```
デバイス(config)# ip igmp snooping querier version 2
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

ip igmp snooping report-suppression

Internet Group Management Protocol (IGMP) レポート抑制をイネーブルにするには、device スタックまたはスタンドアロン device で **ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。IGMP レポート抑制をディセーブルにして、すべての IGMP レポートをマルチキャストルータに転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression
no ip igmp snooping report-suppression

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IGMP レポート抑制はイネーブルです。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IGMP レポート抑制は、マルチキャストクエリに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリに IGMPv3 レポートが含まれている場合はサポートされません。

device は IGMP レポート抑制を使用して、マルチキャストルータクエリごとに 1 つの IGMP レポートのみをマルチキャストデバイスに転送します。IGMP レポート抑制がイネーブル (デフォルト) である場合、device は最初の IGMP レポートをグループのすべてのホストからすべてのマルチキャストルータに送信します。device は、グループの残りの IGMP レポートをマルチキャストルータに送信しません。この機能により、マルチキャストデバイスにレポートが重複して送信されることを防ぎます。

マルチキャストルータクエリに IGMPv1 および IGMPv2 レポートに対する要求のみが含まれている場合、device は最初の IGMPv1 レポートまたは IGMPv2 レポートのみを、グループのすべてのホストからすべてのマルチキャストルータに転送します。マルチキャストルータクエリに IGMPv3 レポートに対する要求も含まれる場合、device はグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャストデバイスに転送します。

no ip igmp snooping report-suppression コマンドを入力して IGMP レポート抑制をディセーブルにした場合、すべての IGMP レポートがすべてのマルチキャストルータに転送されます。

例

次の例では、レポート抑制をディセーブルにする方法を示します。

```
デバイス(config)# no ip igmp snooping report-suppression
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip igmp snooping vlan mrouter

マルチキャストルータポートの追加を行うには、`device`スタックまたはスタンドアロン`device`で **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

Command Default デフォルトでは、マルチキャストルータポートはありません。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

設定は、NVRAM に保存されます。

例

次の例では、ポートをマルチキャストルータポートとして設定する方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

ip igmp snooping vlan static

Internet Group Management Protocol (IGMP) スヌーピングをイネーブルにし、マルチキャストグループのメンバとしてレイヤ 2 ポートをスタティックに追加するには、**device** スタックまたはスタンドアロン **device** で **ip igmp snooping vlan static** グローバル コンフィギュレーション コマンドを使用します。静的マルチキャストグループのメンバとして指定されたポートを削除するには、このコマンドの **no** 形式を使用します。

```
ip igmp snooping vlan vlan-id static ip-address interface interface-id
no ip igmp snooping vlan vlan-id static ip-address interface interface-id
```

Syntax Description	<i>vlan-id</i>	指定した VLAN で IGMP スヌーピングをイネーブルにします。範囲は 1 ~ 1001 および 1006 ~ 4094 です。
	<i>ip-address</i>	指定のグループ IP アドレスを持ったマルチキャストグループのメンバとして、レイヤ 2 ポートを追加します。
	interface <i>interface-id</i>	メンバポートのインターフェイスを指定します。 <i>interface-id</i> には次のオプションがあります。 <ul style="list-style-type: none"> • <i>fastethernet interface number</i>: ファストイーサネット IEEE 802.3 インターフェイス。 • <i>gigabitethernet interface number</i>: ギガビットイーサネット IEEE 802.3z インターフェイス。 • <i>tengigabitethernet interface number</i>: 10 ギガビットイーサネット IEEE 802.3z インターフェイス。 • <i>port-channel interface number</i>: チャンネルインターフェイス。範囲は 0 ~ 128 です。
Command Default	デフォルトでは、マルチキャストグループのメンバとしてスタティックに設定されたポートはありません。	
Command Modes	グローバル コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。 設定は、NVRAM に保存されます。	

例

次の例では、インターフェイス上のホストをスタティックに設定する方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface  
gigabitEthernet1/0/1
```

```
Configuring port gigabitEthernet1/0/1 on group 224.2.4.12
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip multicast auto-enable

IP マルチキャストの認証、許可、およびアカウントリング (AAA) の有効化をサポートするには、**ip multicast auto-enable** コマンドを使用します。このコマンドによって、RADIUS サーバから、AAA 属性を使用しているダイヤルアップインターフェイスでのマルチキャストルーティングを動的に有効化できます。AAA の IP マルチキャストを無効にするには、このコマンドの **no** 形式を使用します。

ip multicast auto-enable
no ip multicast auto-enable

Syntax Description	このコマンドには引数またはキーワードはありません。	
Command Default	なし	
Command Modes	グローバル コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次の例は、IP マルチキャスト上の AAA をイネーブルにする方法を示します。

```
デバイス(config)# ip multicast auto-enable
```

ip multicast-routing

IP マルチキャストルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで **ip multicast-routing** コマンドを使用します。IP マルチキャストルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip multicast-routing [**vrf** *vrf-name*]
no ip multicast-routing [**vrf** *vrf-name*]

Syntax Description

vrf (任意) *vrf-name* 引数に指定されたマルチキャスト VPN ルーティングおよび転送 *vrf-name* (MVRP) インスタンスのための IP マルチキャストルーティングを有効にします。

Command Default

IP マルチキャストルーティングはディセーブルになっています。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IP マルチキャストルーティングがディセーブルになっている場合、Cisco IOS XE ソフトウェアはどのマルチキャストパケットも転送しません。



Note IP-マルチキャストの場合は、IP マルチキャストルーティングを有効にした後に、PIM をすべてのインターフェイスに設定する必要があります。IP マルチキャストルーティングを無効にしても PIM は削除されません。PIM は、インターフェイスの設定から明示的に削除する必要があります。

Examples

次に、IP マルチキャストルーティングをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip multicast-routing
```

次に、特定の VRF の IP マルチキャストルーティングを有効にする例を示します。

```
Device(config)# ip multicast-routing vrf vrf1
```

Related Commands

コマンド	説明
ip pim	インターフェイスに対して PIM をイネーブルにします。

ip pim accept-register

Protocol Independent Multicast (PIM) 登録メッセージをフィルタ処理するように候補ランデブーポイント (RP) スイッチを設定するには、グローバル コンフィギュレーション モードで **ip pim accept-register** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name ] accept-register {list access-list}
no ip pim [vrf vrf-name ] accept-register
```

Syntax Description

vrf vrf-name (任意) *vrf-name* 引数に指定されたマルチキャスト バーチャルプライベート ネットワーク (VPN) ルーティングおよび転送 (MVRF) インスタンスに関連付けられている (S, G) トラフィック用の候補 RP で PIM 登録フィルタを設定します。

list access-list 許可または拒否する PIM 登録メッセージ内の (S, G) トラフィックを定義する数値または名前として、*access-list* 引数を指定します。指定できる範囲は 100 ~ 199 で、拡張された範囲は 2000 ~ 2699 です。IP 名前付きアクセス リストも使用できます。

Command Default

PIM 登録フィルタは設定されていません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

不正な送信元が RP に登録されないようにするには、このコマンドを使用します。不正な送信元が RP に登録メッセージを送信すると、RP はただちに登録停止メッセージを送り返します。

ip pim accept-register コマンドに提供されるアクセスリストは IP 送信元アドレスと IP 宛先アドレスのみをフィルタ処理します。その他のフィールドのフィルタリング (たとえば、IP プロトコルまたは UDP ポート番号) は無効になっています。これらは、共有ツリーの下方の RP からマルチキャストグループメンバに不要なトラフィックを転送する場合があります。より複雑なフィルタリングが必要な場合は、代わりに、**ip multicast boundary** コマンドを使用します。

例

次に、SSM グループ範囲 (232.0.0.0/8) に送信している送信元アドレス 172.16.10.1 を除き、任意のグループ範囲に送信している送信元アドレスの登録パケットを許可する例を示します。これらは拒否されます。候補 RP は最初のホップルータまたはスイッチから PIM 登録を受信するため、これらのステートメントはすべての候補 RP に設定する必要があります。

```
デバイス(config)# ip pim accept-register list ssm-range
デバイス(config)# ip access-list extended ssm-range
デバイス(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
デバイス(config-ext-nacl)# permit ip any any
```

ip pim bsr-candidate

候補 BSR になるようにデバイスを設定するには、グローバル コンフィギュレーション モードで **ip pim bsr-candidate** コマンドを使用します。候補 BSR としてのスイッチを削除するには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] bsr-candidate interface-id [hash-mask-length] [priority]
no ip pim [vrf vrf-name] bsr-candidate
```

Syntax Description

vrf vrf-name	(任意) <i>vrf-name</i> 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク (MVPN) ルーティングおよび転送 (MVRP) インスタンスの候補 BSR になるようにデバイスを設定します。
interface-id	BSR アドレスを候補にするための、そのアドレスの派生元であるデバイスのインターフェイスの ID。このインターフェイスは、 ip pim コマンドを使用して、Protocol Independent Multicast (PIM) に対して有効にする必要があります。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
hash-mask-length	(任意) PIMv2 ハッシュ機能がコールされる前にグループアドレスと論理積をとるマスク長 (最大 32 ビット)。同じシードハッシュを持つグループはすべて、同じランデブーポイント (RP) に対応します。たとえば、マスク長が 24 の場合、グループアドレスの最初の 24 ビットだけが使用されます。ハッシュマスク長により、1つの RP を複数のグループで使用できるようになります。デフォルトのハッシュマスク長は 0 です。
priority	(任意) BSR (C-BSR) 候補のプライオリティ。有効な範囲は 0 ~ 255 です。デフォルトのプライオリティは 0 です。最高のプライオリティ値を持つ C-BSR が優先されます。

Command Default

デバイスはそれ自体を候補 BSR として通知するように設定されていません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast (PIM) に対して有効にする必要があります。

このコマンドは、指定されたインターフェイスのアドレスを BSR アドレスとして示す BSR メッセージをすべての PIM ネイバーに送信するようにデバイスを設定します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーンデバイスで設定する必要があります。

BSR メカニズムは RFC 2362 で指定されています。候補 RP (C-RP) は、ユニキャスト C-RP アドバタイズメント パケットを BSR にスイッチングします。その後、BSR は、これらのアドバタイズメントを BSR メッセージに集約します。BSR メッセージは、TTL 1 で、ALL-PIM-ROUTERS グループのアドレス 224.0.0.13 に定期的にマルチキャストされます。これらのメッセージのマルチキャストは、ホップバイホップ RPF フラッドイングによって処理されます。事前の IP マルチキャストルーティング設定は必要ありません (AutoRP とは異なる)。また、BSR は、特定のグループ範囲について指定された RP を事前を選択しません (AutoRP とは異なる)。代わりに、BSR メッセージを受信する各スイッチが BSR メッセージ内の情報に基づいてグループ範囲の RP を選択します。

シスコ デバイスは BSR メッセージを常に受け入れ、処理します。この機能を無効にするコマンドはありません。

シスコ デバイスは、次の手順で、どの C-RP がグループで使用されているかを判別します。

- BSR C-RP で通知されるグループ プレフィックスに対して最長一致ルックアップを実行します。
- 最長一致ルックアップによって BSR が学習した C-RP が複数見つかった場合は、優先順位が最低の C-RP (`ip pim rp-candidate` コマンドで設定される) が優先されます。
- 複数の BSR が学習した C-RP で優先順位が同じ場合は、グループの RP を選択するために、BSR ハッシュ関数を使用されます。
- 複数の BSR が学習した C-RP が BSR ハッシュ関数から派生された同じハッシュ値を返す場合は、最高の IP アドレスの BSR C-RP が優先されます。

例

次に、ハッシュ マスク長 0 および優先順位 192 を使用して、ギガビットイーサネット インターフェイス 1/0/0 のデバイスの IP アドレスが BSR C-RP になるように設定する例を示します。

```
デバイス(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-candidate

自身を Protocol Independent Multicast (PIM) バージョン 2 (PIMv2) 候補ランデブーポイント (C-RP) として BSR にアドバタイズするように デバイス を設定するには、グローバル コンフィギュレーション モードで **ip pim rp-candidate** コマンドを使用します。C-RP としての デバイス を削除するには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
no ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
```

Syntax Description

vrf <i>vrf-name</i>	(任意) <i>vrf-name</i> 引数に指定されたマルチキャスト バーチャルプライベート ネットワーク (MVPN) ルーティングおよび転送 (MVRF) インスタンスの PIMv2 C-RP として自身を BSR にアドバタイズするようにスイッチを設定します。
<i>interface-id</i>	対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスの ID。有効なインターフェイスは、物理ポート、ポートチャンネル、VLAN などです。
group-list <i>access-list-number</i>	(任意) RP アドレスに関連してアドバタイズされるグループプレフィックスを定義する標準 IP アクセス リスト番号を指定します。

Command Default

デバイスは PIMv2 C-RP として自身を BSR に通知するように設定されていません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

自身を候補 RP として BSR アドバタイズするために PIMv2 メッセージを送信するように デバイス を設定するには、このコマンドを使用します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーンデバイスで設定する必要があります。

interface-id によって指定されたインターフェイスに関連付けられている IP アドレスは C-RP アドレスとしてアドバタイズされます。

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast (PIM) に対して有効にする必要があります。

オプションの **group-list** キーワードと *access-list-number* 引数が設定されている場合は、RP アドレスとのアソシエーション時に、標準 IP アクセスリストによって定義されたグループプレフィックスもアドバタイズされます。

例

次に、自身を C-RP として PIM ドメイン内の BSR にアドバタイズするようにスイッチを設定する例を示します。標準アクセスリスト番号 4 により、ギガビットイーサネットインターフェイス 1/0/1 で識別されるアドレスを持つ RP に対応するグループプレフィックスが指定されます。

```
デバイス(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

Auto-RP を使用して、デバイスがランデブーポイント（RP）として動作するグループを設定するには、グローバル コンフィギュレーション モードで **ip pim send-rp-announce** コマンドを使用します。デバイスの RP としての設定を解除するには、このコマンドの **no** 形式を使用します。

```
ip pim [vrf vrf-name] send-rp-announce interface-id scope ttl-value [group-list access-list-number]
[interval seconds]
no ip pim [vrf vrf-name] send-rp-announce interface-id
```

Syntax Description

vrf vrf-name	（任意）デバイスがランデブーポイント（RP）として動作するグループを設定するには、 <i>vrf-name</i> 引数に Auto-RP を使用します。
interface-id	RP アドレスを識別するインターフェイスのインターフェイス ID を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
scope ttl-value	Auto-RP アナウンスメントの数を制限するホップでの存続可能時間（TTL）を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに確実に到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。範囲は 1 ～ 255 です。
group-list access-list-number	（任意）RP アドレスに関連してアドバタイズされるグループプレフィックスを定義する標準 IP アクセス リスト番号を指定します。IP 標準アクセス リスト番号を入力します。指定できる範囲は 1 ～ 99 です。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。
interval seconds	（任意）RP アナウンスメント間の間隔を秒単位で指定します。RP アナウンスメントの合計保留時間は、間隔値の 3 倍に自動設定されます。デフォルトインターバルは 60 秒です。範囲は 1 ～ 16383 です。

Command Default

Auto-RP はディセーブルです。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

RP にするデバイスで次のコマンドを入力します。Auto-RP を使用してグループ/RP マッピングを配信すると、ルータはこのコマンドにより既知のグループ CISCO-RP-ANNOUNCE (224.0.1.39) に Auto-RP アナウンスメント メッセージを送信します。このメッセージは、ルータがアクセス リストで規定される範囲内のグループに対する候補 RP であることを通知します。

このコマンドは、双方向転送を行う場合、および Auto-RP を使用してグループ/RP のマッピングを分散する場合に、**bidir** キーワードを指定して使用します。他のオプションは、次のとおりです。

- PIM バージョン 2 ブートストラップルータ（PIMv2 BSR）メカニズムによりグループ/RP のマッピングを分散する場合は、**ip pim rp-candidate** コマンドで **bidir** キーワードを使用します。
- Auto-RP または PIMv2 BSR メカニズムのどちらによってもグループ/RP のマッピングを分散しない場合は、**ip pim rp-address** コマンドで **bidir** キーワードを使用します。

例

次に、最大 31 ホップのすべての Protocol Independent Multicast（PIM）対応インターフェイスに RP アナウンスメントを送信するようにデバイスを設定する例を示します。スイッチを RP として識別するために使用される IP アドレスは、120 秒間隔でギガビットイーサネットインターフェイス 1/0/1 に関連付けられる IP アドレスです。

```
Device(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5 interval 120
```

ip pim snooping

Protocol Independent Multicast (PIM) スヌーピングをグローバルに有効にするには、グローバル コンフィギュレーション モードで **ip pim snooping** コマンドを使用します。PIM スヌーピングをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

ip pim snooping
no ip pim snooping

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default PIM スヌーピングは有効になっていません。

Command Modes グローバル コンフィギュレーション

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）をエイリアスとして使用するグループでは、PIM スヌーピングはサポートされません。

PIM スヌーピングをグローバルにディセーブルにすると、PIM スヌーピングはすべての VLAN 上でディセーブルになります。

Examples

次の例は、PIM スヌーピングをグローバルにイネーブルにする方法を示します。

```
ip pim snooping
```

次の例は、PIM スヌーピングをグローバルにディセーブルにする方法を示します。

```
no ip pim snooping
```

コマンド	説明
clear ip pim snooping	インターフェイス上の PIM スヌーピングを削除します。
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping dr-flood

指定ルータへのパケットのフラッディングを有効にするには、グローバル コンフィギュレーション モードで **ip pim snooping dr-flood** コマンドを使用します。指定ルータへのパケットのフラッディングを無効にするには、このコマンドの **no** 形式を使用します。

ip pim snooping dr-flood
no ip pim snooping dr-flood

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default 指定ルータへのパケットのフラッディングは、デフォルトでは有効になっています。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）をエイリアスとして使用するグループでは、PIM スヌーピングはサポートされません。

no ip pim snooping dr-flood コマンドは、指定ルータが接続されていないスイッチ上でのみ入力します。

指定ルータは、（S,G）O リストで自動的にプログラムされます。

Examples

次に、指定ルータへのパケットのフラッディングをイネーブルにする例を示します。

```
ip pim snooping dr-flood
```

次に、指定ルータへのパケットのフラッディングをディセーブルにする例を示します。

```
no ip pim snooping dr-flood
```

Related Commands	コマンド	説明
	clear ip pim snooping	インターフェイス上のPIM スヌーピングを削除します。
	show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping vlan

インターフェイスで Protocol Independent Multicast (PIM) スヌーピングを有効にするには、グローバル コンフィギュレーション モードで **ip pim snooping vlan** コマンドを使用します。PIM スヌーピングをインターフェイスで無効にするには、このコマンドの **no** 形式を使用します。

ip pim snooping vlan *vlan-id*
no ip pim snooping vlan *vlan-id*

Syntax Description

<i>vlan-id</i>	VLAN ID 値。範囲は 1 ~ 1001 です。先頭の 0 は入力しないでください。
----------------	--

Command Default

PIM スヌーピングはインターフェイスで無効になっています。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）をエイリアスとして使用するグループでは、PIM スヌーピングはサポートされません。

このコマンドは、未設定の VLAN を自動的に設定します。設定は、NVRAM に保存されます。

Examples

次に、VLAN インターフェイス上で PIM スヌーピングをイネーブルにする例を示します。

```
Router(config)# ip pim snooping vlan 2
```

次に、VLAN インターフェイス上で PIM スヌーピングをディセーブルにする例を示します。

```
Router(config)# no ip pim snooping vlan 2
```

Related Commands

コマンド	説明
clear ip pim snooping	インターフェイス上の PIM スヌーピングを削除します。
ip pim snooping	PIM スヌーピングをグローバルにイネーブルにします。
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim spt-threshold

最短パスツリー (spt) に移行する上限値となるしきい値を指定するには、グローバル コンフィギュレーションモードで **ip pim spt-threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。

```
ip pim {kpbs | infinity} [group-list access-list]
no ip pim {kpbs | infinity} [group-list access-list]
```

Syntax Description	<i>kpbs</i>	最短パスツリー (spt) に移行する上限値となるしきい値を指定します。有効な範囲は 0 ~ 4294967 ですが、0 が唯一有効なエントリです。0 エントリは、常に送信元ツリーに切り替わります。
	infinity	指定されたグループのすべての送信元が共有ツリーを使用し、送信元ツリーに切り替わらないように指定します。
	group-list access-list	(任意) アクセスリスト番号を指定するか、または作成した特定のアクセスリストを名前指定します。値 0 を指定する場合、または group-list access-list オプションを使用しない場合、しきい値はすべてのグループに適用されません。
Command Default	PIM 最短パス ツリー (spt) に切り替わります。	
Command Modes	グローバル コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、アクセス リスト 16 のすべての送信元が共有ツリーを使用するように指定する例を示します。

```
デバイス(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

サービス リストを照合するメッセージタイプを設定するには、**match message-type** コマンドを使用します。

```
match message-type {announcement |any |query}
```

Syntax Description	<p>announcement デバイスのサービス アドバタイズメントまたはアナウンスメントのみを許可します。</p> <p>any 任意の照合タイプを許可します。</p> <p>query ネットワーク内の特定のデバイスに対するクライアントからクエリのみを許可します。</p>
Command Default	なし
Command Modes	サービス リスト コンフィギュレーション。
Command History	<p>リリー 変更内容</p> <p>ス</p> <p>このコマンドが導入されました。</p>

Usage Guidelines 異なるシーケンス番号を持つ同じ名前の複数のサービス マップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション **permit** または **deny** が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは **deny** です。



Note **service-list mdns-sd service-list-name query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合されるアナウンスメント メッセージタイプを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match message-type announcement
```

match service-type

照合する mDNS サービス タイプ文字列値を設定するには、**match service-type** コマンドを使用します。

match service-type *line*

Syntax Description	<i>line</i> パケット内のサービスタイプを照合するための正規表現。
Command Default	なし
Command Modes	サービス リスト コンフィギュレーション
Command History	リリー 変更内容 ス このコマンドが導入されました。

Usage Guidelines **service-list mdns-sd service-list-name query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合する mDNS サービス タイプ文字列値を設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match service-instance

サービス リストを照合するサービス インスタンスを設定するには、**match service-instance** コマンドを使用します。

match service-instance *line*

Syntax Description

line パケット内のサービス インスタンスを照合するための正規表現。

Command Default

なし

Command Modes

サービス リスト コンフィギュレーション

Command History

リリー 変更内容
ス

このコマンドが導入されました。

Usage Guidelines

service-list mdns-sd service-list-name query コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合するサービス インスタンスを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-instance servInst 1
```

mrinfo

ピアとして動作している隣接するマルチキャストルータまたはマルチレイヤスイッチをクエリするには、ユーザ EXEC モードまたは特権 EXEC モードで **mrinfo** コマンドを使用します。

mrinfo [**vrf** *route-name*] [*hostname* | *address*] [*interface-id*]

Syntax Description

vrf <i>route-name</i>	(任意) VPN ルーティングおよび転送インスタンスを指定します。
<i>hostname</i> <i>address</i>	(任意) クエリするマルチキャストルータまたはマルチレイヤスイッチのドメインネームシステム (DNS) 名または IP アドレス。省略すると、スイッチは自身をクエリします。
<i>interface-id</i>	(任意) インターフェイス ID。

Command Default

このコマンドはディセーブルです。

Command Modes

ユーザ EXEC
特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

mrinfo コマンドは、マルチキャストルータまたはスイッチのピアとして動作している隣接するマルチキャストルータまたはスイッチを判別するためのマルチキャストバックボーン (MBONE) のオリジナルのツールです。シスコルータは、Cisco IOS リリース 10.2 から **mrinfo** 要求をサポートしています。

mrinfo コマンドを使用して、マルチキャストルータまたはマルチレイヤスイッチをクエリすることができます。出力フォーマットは、マルチキャストルーテッドバージョンのディスタンスベクターマルチキャストルーティングプロトコル (DVMRP) と同じです (mrouted ソフトウェアは、DVMRP を実装する UNIX ソフトウェアです)。

例

次に、**mrinfo** コマンドの出力例を示します。

```
デバイス# mrinfo
vrf 192.0.1.0
192.31.7.37 (barnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```



Note フラグの意味は次のとおりです。

- P: プルーニング対応
 - M: mtrace 対応
 - S: シンプル ネットワーク管理プロトコルに対応
 - A: Auto RP に対応
-

service-policy-query

サービスリストクエリの周期を設定するには、**service-policy-query** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

service-policy-query [*service-list-query-name service-list-query-periodicity*]
no service-policy-query

Syntax Description	<i>service-list-query-name service-list-query-periodicity</i> (任意) サービスリストクエリの周期。
---------------------------	---

Command Default	ディセーブル
------------------------	--------

Command Modes	mDNS コンフィギュレーション
----------------------	------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	<p>非要求アナウンスメントを送信しないデバイスがあるため、そのようなデバイスにサービスを強制的に学習させ、それらをキャッシュ内で最新に維持するために、このコマンドには、アクティブクエリリストに一覧されているサービスが確実にクエリされるようにするアクティブクエリ機能が含まれています。</p>
-------------------------	--

例

次に、サービスリストのクエリの周期を設定する例を示します。

```
デバイス(config-mdns)# service-policy-query sl-query1 100
```

service-policy

サービスリストの着信または発信サービス検出情報にフィルタを適用するには、**service-policy** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

```
service-policy service-policy-name {IN | OUT}  
no service-policy service-policy-name {IN | OUT}
```

Syntax Description	IN 着信サービス検出情報にフィルタを適用します。				
	OUT 発信サービス検出情報にフィルタを適用します。				
Command Default	ディセーブル				
Command Modes	mDNS コンフィギュレーション				
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Fuji 16.9.2</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

例

次の例に、サービス リストの着信サービス検出情報にフィルタを適用する方法を示します。

```
デバイス(config-mdns)# service-policy serv-pol1 IN
```

show ip igmp filter

Internet Group Management Protocol (IGMP) フィルタ情報を表示するには、特権 EXEC モードで **show ip igmp filter** コマンドを使用します。

show ip igmp [**vrf** *vrf-name*] **filter**

Syntax Description	vrf <i>vrf-name</i> (任意) マルチキャスト VPN ルーティングおよび転送 (VRF) インスタンスをサポートします。				
Command Default	IGMP フィルタはデフォルトで有効になっています。				
Command Modes	特権 EXEC				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	show ip igmp filter コマンドは、device に定義されているすべてのフィルタに関する情報を表示します。				

例

次に、**show ip igmp filter** コマンドの出力例を示します。

```
デバイス# show ip igmp filter
```

```
IGMP filter enabled
```

show ip igmp profile

設定済みのすべての Internet Group Management Protocol (IGMP) プロファイルまたは指定された IGMP プロファイルを表示するには、特権 EXEC モードで **show ip igmp profile** コマンドを使用します。

```
show ip igmp [vrf vrf-name] profile [profile number]
```

Syntax Description	vrf vrf-name (任意) マルチキャスト VPN ルーティングおよび転送 (VRF) インスタンスをサポートします。				
	profile number (任意) 表示する IGMP プロファイル番号。指定できる範囲は 1 ~ 4294967295 です。プロファイル番号が入力されていない場合、すべての IGMP プロファイルが表示されます。				
Command Default	IGMP プロファイルはデフォルトでは定義されていません。				
Command Modes	特権 EXEC				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	なし				

例

次に、device のプロファイル番号 40 に対する **show ip igmp profile** コマンドの出力例を示します。

```
デバイス# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255
```

次に、device に設定されているすべてのプロファイルに対する **show ip igmp profile** コマンドの出力例を示します。

```
デバイス# show ip igmp profile

IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
  range 229.9.9.0 229.255.255.255
```

show ip igmp snooping

deviceまたはVLANのInternet Group Management Protocol (IGMP) スヌーピング構成を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip igmp snooping** コマンドを使用します。

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

Syntax Description	groups	(任意) IGMP スヌーピング マルチキャスト テーブルを表示します。
Command Default	なし	
Command Modes	ユーザ EXEC 特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	<p>VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。</p> <p>文字列では、大文字と小文字が区別されます。たとえば、「 exclude output」と入力した場合、「output」を含む行は表示されませんが、「Output」を含む行は表示されます。</p>	

例

次に、**show ip igmp snooping vlan 1** コマンドの出力例を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
デバイス# show ip igmp snooping vlan 1
```

```
Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
```

```

Robustness variable      : 2
Last member query count  : 2
Last member query interval : 1000

```

```
Vlan 1:
```

```

-----
IGMP snooping              : Enabled
IGMPv2 immediate leave     : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode  : IGMP_ONLY
Robustness variable        : 2
Last member query count    : 2
Last member query interval  : 1000

```

次に、**show ip igmp snooping** コマンドの出力例を示します。ここでは、device 上のすべての VLAN のスヌーピング特性を表示します。

```
デバイス# show ip igmp snooping
```

```
Global IGMP Snooping configuration:
```

```

-----
IGMP snooping              : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2
Robustness variable       : 2
Last member query count   : 2
Last member query interval : 1000

```

```
Vlan 1:
```

```

-----
IGMP snooping              : Enabled
IGMPv2 immediate leave     : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode  : IGMP_ONLY
Robustness variable        : 2
Last member query count    : 2
Last member query interval  : 1000

```

```
Vlan 2:
```

```

-----
IGMP snooping              : Enabled
IGMPv2 immediate leave     : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode  : IGMP_ONLY
Robustness variable        : 2
Last member query count    : 2
Last member query interval  : 1000

```

```

-
.
.
.

```

show ip igmp snooping groups

device またはマルチキャスト情報の Internet Group Management Protocol (IGMP) スヌーピング マルチキャスト テーブルを表示するには、特権 EXEC モードで **show ip igmp snooping groups** コマンドを使用します。

Command Modes
特権 EXEC
ユーザ EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 文字列では、大文字と小文字が区別されます。たとえば、「**exclude output**」と入力した場合、「**output**」を含む行は表示されませんが、「**Output**」を含む行は表示されます。

例

次に、キーワードを指定しない **show ip igmp snooping groups** コマンドの出力例を示します。device のマルチキャストテーブルが表示されます。

```
デバイス# show ip igmp snooping groups
```

Vlan	Group	Type	Version	Port List
1	224.1.4.4	igmp		Gi1/0/11
1	224.1.4.5	igmp		Gi1/0/11
2	224.0.1.40	igmp	v2	Gi1/0/15
104	224.1.4.2	igmp	v2	Gi2/0/1, Gi2/0/2
104	224.1.4.3	igmp	v2	Gi2/0/1, Gi2/0/2

次に、**show ip igmp snooping groups count** コマンドの出力例を示します。device 上のマルチキャスト グループの総数が表示されます。

```
デバイス# show ip igmp snooping groups count
```

```
Total number of multicast groups: 2
```

次に、**show ip igmp snooping groups vlan vlan-id ip-address** コマンドの出力例を示します。指定された IP アドレスのグループのエントリを表示します。

```
デバイス# show ip igmp snooping groups vlan 104 224.1.4.2
```

Vlan	Group	Type	Version	Port List
104	224.1.4.2	igmp	v2	Gi2/0/1, Gi1/0/15

show ip igmp snooping mrouter

deviceまたは指定されたマルチキャスト VLAN の Internet Group Management Protocol (IGMP) スヌーピングの動的に学習され、手動で設定されたマルチキャストルータポートを表示するには、特権 EXEC モードで **show ip igmp snooping mrouter** コマンドを使用します。

show ip igmp snooping mrouter [*vlan vlan-id*]

Syntax Description

vlan *vlan-id* (任意) VLAN を指定します。範囲は 1 ~ 1001 と 1006 ~ 4094 です。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

マルチキャスト VLAN レジストレーション (MVR) がイネーブルの場合、**show ip igmp snooping mrouter** コマンドは MVR マルチキャストルータの情報および IGMP スヌーピング情報を表示します。

式では大文字と小文字が区別されます。たとえば、「|exclude output」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、**show ip igmp snooping mrouter** コマンドの出力例を示します。deviceのマルチキャストルータポートを表示する方法を示します。

```
デバイス# show ip igmp snooping mrouter
```

```
Vlan      ports
----      -
1         Gi2/0/1 (dynamic)
```

show ip igmp snooping querier

device で設定されている IGMP クエリアの設定と操作情報を表示するには、ユーザ EXEC モードで **show ip igmp snooping querier** コマンドを使用します。

show ip igmp snooping querier [vlan *vlan-id*] [detail]

Syntax Description	vlan <i>vlan-id</i> (任意) VLAN を指定します。範囲は 1 ~ 1001 と 1006 ~ 4094 です。	
	detail (任意) IGMP クエリアの詳細情報を表示します。	
Command Modes	ユーザ EXEC	
	特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines IGMP クエリ メッセージを送信する検出デバイス (クエリアとも呼ばれます) の IGMP バージョンと IP アドレスを表示するには、**show ip igmp snooping querier** コマンドを使用します。サブネットは複数のマルチキャストルータを保有できますが、IGMP クエリアは 1 つしか保有できません。IGMPv2 を実行しているサブネットでは、マルチキャストルータの 1 つがクエリアとして設定されます。クエリアには、レイヤ 3 device を指定できます。

show ip igmp snooping querier コマンド出力では、クエリアが検出された VLAN およびインターフェイスも表示されます。クエリアが device の場合、出力の Port フィールドには「Router」と表示されます。クエリアがルータの場合、出力の Port フィールドにはクエリアを学習したポート番号が表示されます。

show ip igmp snooping querier detail ユーザ EXEC コマンドは、**show ip igmp snooping querier** コマンドに似ています。ただし、**show ip igmp snooping querier** コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのみが表示されます。

show ip igmp snooping querier detail コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのほか、次の追加情報が表示されます。

- VLAN で選択されている IGMP クエリア
- VLAN で設定された device クエリア (存在する場合) に関連する設定情報と動作情報

式では大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、**show ip igmp snooping querier** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11    v3                 Gil/0/1
2         172.20.40.20    v2                 Router
```

次に、**show ip igmp snooping querier detail** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier detail

Vlan      IP Address      IGMP Version      Port
-----
1         1.1.1.1         v2                 Fa8/0/1
Global IGMP device querier status

-----
admin state           : Enabled
admin version         : 2
source IP address     : 0.0.0.0
query-interval (sec)  : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10
Vlan 1: IGMP device querier status

-----
elected querier is 1.1.1.1          on port Fa8/0/1

-----
admin state           : Enabled
admin version         : 2
source IP address     : 10.1.1.65
query-interval (sec)  : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10
operational state     : Non-Querier
operational version   : 2
tcn query pending count : 0
```

show ip pim autorp

Auto-RP に関するグローバル情報を表示するには、特権 EXEC モードで **show ip pim autorp** コマンドを使用します。

show ip pim autorp

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default Auto RP は、デフォルトでは有効になっています。

Command Modes 特権 EXEC

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、Auto-RP が有効になっているか、無効になっているかを表示します。

例

次に、Auto-RP が有効になっている場合のコマンドの出力例を示します。

```
デバイス# show ip pim autorp
```

```
AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.
```

```
PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

show ip pim bsr-router

Protocol Independent Multicast (PIM) ブートストラップルータ (BSR) プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr-router** コマンドを使用します。

show ip pim bsr-router

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

なし

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Auto-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドで BSR ルータの情報が表示されます。

次に、**show ip pim bsr-router** コマンドの出力例を示します。

```
デバイス# show ip pim bsr-router
```

```
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

Protocol Independent Multicast (PIM) ブートストラップルータ (BSR) プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr** コマンドを使用します。

show ip pim bsr

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes ユーザ EXEC
特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines Auto-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドで BSR ルータの情報が表示されます。

次に、**show ip pim bsr** コマンドの出力例を示します。

```

デバイス# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6

```

show ip pim snooping

IP PIM スヌーピングに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim snooping** コマンドを使用します。

Global Status

show ip pim snooping

VLAN Status

show ip pim snooping vlan *vlan-id* [**neighbor** | **statistics** | **mroute** [*source-ipgroup-ip*]]

Syntax Description

vlan <i>vlan-id</i>	特定の VLAN の情報を表示します。有効な値は 1 ~ 4094 です。
neighbor	(任意) 近接データベースに関する情報を表示します。
statistics	(任意) VLAN 統計情報を表示します。
mroute	(任意) mroute データベースに関する情報を表示します。
<i>source-ip</i>	(任意) 送信元 IP アドレス。
<i>group-ip</i>	(任意) グループ IP アドレス。

Command Default

このコマンドには、デフォルト設定がありません。

Command Modes

ユーザ EXEC、特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、グローバルステータスに関する情報を表示する例を示します。

```
Router# show ip pim snooping

Global runtime mode: Enabled
Global admin mode   : Enabled
DR Flooding status  : Disabled
SGR-Prune Suppression: Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 1001
```

次に、特定の VLAN に関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 1001

4 neighbors (0 DR priority incapable, 4 Bi-dir incapable)
5000 mroutes, 0 mac entries
DR is 10.10.10.4
```

```
RP DF Set:
QinQ snooping : Disabled
```

次に、特定の VLAN の近接データベースに関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 1001 neighbor
```

IP Address	Mac address	Port	Uptime/Expires	Flags
VLAN 1001: 3 neighbors				
10.10.10.2	000a.f330.344a	Po128	02:52:27/00:01:41	
10.10.10.1	000a.f330.334a	Hu1/0/7	04:54:14/00:01:38	
10.10.10.4	000a.f330.3c00	Hu1/0/1	04:53:45/00:01:34	DR

次に、特定の VLAN の詳細統計情報を表示する例を示します。

```
Router# show ip pim snooping vlan 1001 statistics
```

```
PIMv2 statistics:
Total : 56785
Process Enqueue : 56785
Process PIMv2 input queue current outstanding : 0
Process PIMv2 input queue max size reached : 110
Error - Global Process State not RUNNING : 0
Error - Process Enqueue : 0
Error - Drops : 0
Error - Bad packet floods : 0
Error - IP header generic error : 0
Error - IP header payload len too long : 0
Error - IP header payload len too short : 0
Error - IP header checksum : 0
Error - IP header dest ip not 224.0.0.13 : 0
Error - PIM header payload len too short : 0
Error - PIM header checksum : 0
Error - PIM header checksum in Registers : 0
Error - PIM header version not 2 : 0
```

次に、特定の VLAN におけるすべてのマルチキャストルータの mroute データベースに関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mroute
```

```
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
SGR-P - (S,G,R) Prune

VLAN 1001: 5000 mroutes
(*, 225.0.1.0), 00:14:54/00:02:59
 10.10.10.120->10.10.10.105, 00:14:54/00:02:59, J
  Downstream ports: Po128
  Upstream ports: Hu1/0/7
  Outgoing ports: Hu1/0/7 Po128

(11.11.11.10, 225.0.1.0), 00:14:54/00:02:59
 10.10.10.130->10.10.10.120, 00:14:54/00:02:59, SGR-P
  Downstream ports:
  Upstream ports: Hu1/0/7
  Outgoing ports:

(*, 225.0.5.0), 00:14:53/00:02:57
 10.10.10.105->10.10.10.10, 00:14:53/00:02:57, J
  Downstream ports: Po128
  Upstream ports: Hu1/0/7
  Outgoing ports: Hu1/0/7 Po128
```

```
(11.11.11.10, 225.0.5.0), 00:14:53/00:02:57
 10.10.10.105->10.10.10.130, 00:14:53/00:02:57, SGR-P
 Downstream ports:
 Upstream ports: Hu1/0/7
 Outgoing ports:
 Number of matching mroutes found: 4
```

次に、特定の送信元アドレスの PIM mroute に関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mroute 172.16.100.100
```

```
(*, 172.16.100.100), 00:16:36/00:02:36
 10.10.10.1->10.10.10.2, 00:16:36/00:02:36, J
 Downstream ports: 3/12
 Upstream ports: 3/13
 Outgoing ports: 3/12 3/13
```

次に、特定の送信元アドレスおよびグループアドレスの PIM mroute に関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mroute 192.168.0.0 172.16.10.10
```

```
(192.168.0.0, 172.16.10.10), 00:03:04/00:00:25
 10.10.10.1->10.10.10.2, 00:03:04/00:00:25, j
 Downstream ports: 3/12
 Upstream ports: 3/13
 Outgoing ports: 3/12 3/13
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 97: show ip pim snooping のフィールドの説明

フィールド	説明
Downstream ports	PIM が参加しているポートが受信されました。
Upstream ports	RP と送信元に向かうポート。
Outgoing ports	マルチキャストフローのすべてのアップストリーム ポートおよびダウンストリーム ポートのリスト。

Related Commands

コマンド	説明
clear ip pim snooping vlan	インターフェイス上の PIM スヌーピングを削除します。
ip pim snooping	PIM スヌーピングをグローバルにイネーブルにします。
ip pim snooping vlan	インターフェイス上の PIM スヌーピングをイネーブルにします。

show ip pim tunnel

インターフェイス上の Protocol Independent Multicast (PIM) レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示するには、 **show ip pim tunnel** コマンドを使用します。

show ip pim [*vrf vrf-name*] **tunnel** [*Tunnel interface-number* | **verbose**]

Syntax Description	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	Tunnel <i>interface-number</i>	(任意) トンネルインターフェイス番号を指定します。
	verbose	(任意) MACカプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報を表示します。
Command Default	なし	
Command Modes	特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines PIM トンネルインターフェイスに関する情報を表示するには、 **show ip pim tunnel** を使用します。

PIM トンネルインターフェイスは、PIM スパースモード (PIM-SM) 登録プロセスの IPv4 マルチキャスト転送情報ベース (MFIB) で使用されます。IPv4 MFIB では、2 種類の PIM トンネルインターフェイスが使用されます。

- PIM カプセル化トンネル (PIM Encap トンネル)
- PIM カプセル化解除トンネル (PIM Decap トンネル)

PIM Encap トンネルは、(Auto-RP、ブートストラップルータ (BSR)、またはスタティック RP の設定を介して) グループからランデブーポイント (RP) へのマッピングを学習するたびに動的に作成されます。PIM Encap トンネルは、送信元が直接接続されているファーストホップ代表ルータ (DR) から送信されるマルチキャストパケットをカプセル化するために使用されます。

PIM Encap トンネルと同様、PIM Decap トンネルインターフェイスは動的に作成されますが、グループから RP へのマッピングを学習するたびに RP 上でのみ作成されます。PIM Decap トンネルインターフェイスは、PIM レジスタのカプセル化解除メッセージのために RP によって使用されます。



Note PIM トンネルは実行コンフィギュレーションには表示されません。

PIM トンネル インターフェイスが作成されると、次の syslog メッセージが表示されます。

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

次に、RP から取得した **show ip pim tunnel** の出力例を示します。この出力は、RP 上の PIM Encap および Decap トンネルを確認するために使用されます。

```
デバイス# show ip pim tunnel
```

```
Tunnel0
  Type   : PIM Encap
  RP     : 70.70.70.1*
  Source: 70.70.70.1
Tunnel1*
  Type   : PIM Decap
  RP     : 70.70.70.1*
  Source: -R2#
```



Note アスタリスク (*) は、そのルータが RPであることを示します。RP には、PIM Encap トンネル インターフェイスおよび PIM Decap トンネル インターフェイスが常にあるとは限りません。

show platform software fed switch ip multicast

プラットフォーム依存IPマルチキャストテーブルおよびその他の情報を表示するには、特権EXECモードで **show platform software fed switch ip multicast** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby**} **ip multicast** {**groups** | **hardware**[**detail**] | **interfaces** | **retry**}

Syntax Description

switch { <i>switch_num</i> active standby }	<p>情報を表示するデバイス。</p> <ul style="list-style-type: none"> • active: アクティブスイッチの情報を表示します。 • standby: 存在する場合、スタンバイスイッチの情報を表示します。
groups	グループごとの IP マルチキャスト ルートを表示します。
hardware [detail]	ハードウェアにロードされた IP マルチキャスト ルートを表示します。任意指定の detail キーワードは、宛先インデックスおよびルートインデックスのポートメンバを表示するために使用します。
interfaces	IP マルチキャスト インターフェイスを表示します。
retry	リトライ キューの IP マルチキャスト ルートを表示します。

Command Modes

特権 EXEC

Command History

リリース	変更内容
	このコマンドが導入されました。

Usage Guidelines

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

例

次に、グループごとのプラットフォーム IP マルチキャスト ルートを表示する例を示します。

```
デバイス# show platform software fed active ip multicast groups
```

```
Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6 flags: C
No RPF interface.
Number of OIF: 0
```

```
Flags: 0x10   Pkts : 0
OIF Details:No OIF interface.

DI details
-----
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f6  index1:0x51f6

Cookie length 56
0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
-----

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
-----

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
```

```
show platform software fed switch ip multicast
```

```
=====
```

```
<output truncated>
```



PART VI

レイヤ 2/3

- [レイヤ 2/3 コマンド](#), on page 795



レイヤ 2/3 コマンド

- [channel-group](#), on page 798
- [channel-protocol](#), on page 802
- [clear l2protocol-tunnel counters](#), on page 803
- [clear lacp](#), on page 804
- [clear pagp](#), on page 805
- [clear spanning-tree counters](#), on page 806
- [clear spanning-tree detected-protocols](#), on page 807
- [debug etherchannel](#), on page 808
- [debug lacp](#), on page 809
- [debug pagp](#), on page 810
- [debug platform pm](#), on page 811
- [debug platform udd](#), on page 813
- [debug spanning-tree](#), on page 814
- [instance \(VLAN\)](#), on page 816
- [interface port-channel](#), on page 818
- [l2protocol-tunnel](#), on page 820
- [lacp fast-switchover](#), on page 824
- [lacp max-bundle](#), on page 826
- [lacp port-priority](#), on page 827
- [lacp rate](#), on page 829
- [lacp system-priority](#), on page 830
- [loopdetect](#), on page 831
- [name \(MST\)](#), on page 834
- [pagp learn-method](#), on page 835
- [pagp port-priority](#), on page 837
- [port-channel](#), on page 838
- [port-channel auto](#), on page 839
- [port-channel load-balance](#), on page 840
- [port-channel load-balance extended](#), on page 842
- [port-channel min-links](#), on page 844
- [rep admin vlan](#), on page 845
- [rep block port](#), on page 846
- [rep lsl-age-timer](#), on page 848

- rep lsl-retries, on page 849
- rep preempt delay, on page 850
- rep preempt segment, on page 852
- rep segment, on page 854
- rep stcn, on page 856
- revision, on page 857
- show dot1q-tunnel, on page 859
- show etherchannel, on page 860
- show interfaces rep detail, on page 863
- show l2protocol-tunnel, on page 865
- show lacp, on page 867
- show loopdetect, on page 872
- show pagp, on page 873
- show platform etherchannel, on page 875
- show platform pm, on page 876
- show rep topology, on page 877
- show spanning-tree, on page 879
- show spanning-tree mst, on page 886
- show udd, on page 889
- spanning-tree backbonefast, on page 893
- spanning-tree bpdupfilter, on page 894
- spanning-tree bpduguard, on page 896
- spanning-tree bridge assurance, on page 898
- spanning-tree cost, on page 900
- spanning-tree etherchannel guard misconfig, on page 902
- spanning-tree extend system-id, on page 904
- spanning-tree guard, on page 905
- spanning-tree link-type, on page 906
- spanning-tree loopguard default, on page 908
- spanning-tree mode, on page 909
- spanning-tree mst, on page 910
- spanning-tree mst configuration, on page 911
- spanning-tree mst forward-time, on page 913
- spanning-tree mst hello-time, on page 914
- spanning-tree mst max-age, on page 915
- spanning-tree mst max-hops, on page 916
- spanning-tree mst pre-standard, on page 917
- spanning-tree mst priority, on page 919
- spanning-tree mst root, on page 920
- spanning-tree mst simulate pvst global, on page 922
- spanning-tree pathcost method, on page 923
- spanning-tree port-priority, on page 924
- spanning-tree portfast edge bpdupfilter default, on page 926
- spanning-tree portfast edge bpduguard default, on page 928
- spanning-tree portfast default, on page 929
- spanning-tree transmit hold-count, on page 931

- spanning-tree uplinkfast, on page 933
- spanning-tree vlan, on page 934
- switchport, on page 937
- switchport access vlan, on page 939
- switchport mode, on page 940
- switchport nonegotiate, on page 943
- switchport voice vlan, on page 945
- udld, on page 948
- udld port, on page 950
- udld reset, on page 952
- vlan dot1q tag native, on page 953

channel-group

EtherChannel グループにイーサネットポートを割り当てる、EtherChannel モードをイネーブルにする、またはその両方を行うには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用します。EtherChannel グループからイーサネットポートを削除するには、このコマンドの **no** 形式を使用します。

channel-group *channel-group-number* **mode** {**active** | **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** | **passive**}

no channel-group

Syntax Description		
	<i>channel-group-number</i>	チャネルグループ番号。 指定できる範囲は 1 ～ 48 です。
	mode	EtherChannel モードを指定します。
	active	無条件に Link Aggregation Control Protocol (LACP) をイネーブルにします。
	auto	Port Aggregation Protocol (PAgP) 装置が検出された場合に限り、PAgP をイネーブルにします。
	non-silent	(任意) PAgP 対応のパートナーに接続されたとき、インターフェイスを非サイレント動作に設定します。他の装置からのトラフィックが予想されている場合に PAgP モードで auto または desirable キーワードとともに使用されます。
	desirable	無条件に PAgP をイネーブルにします。
	on	on モードをイネーブルにします。
	passive	LACP 装置が検出された場合に限り、LACP をイネーブルにします。

Command Default

チャンネルグループは割り当てることができません。
モードは設定されていません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

レイヤ2のEtherChannelでは、チャンネルグループに最初の物理ポートが追加されると、**channel-group** コマンドがポートチャンネル インターフェイスを自動的に作成します。ポートチャンネル インターフェイスを手動で作成するためにグローバルコンフィギュレーションモードで**interface port-channel** コマンドを使用する必要はありません。最初にポートチャンネル インターフェイスを作成する場合は、**channel-group-number** を **port-channel-number** と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャンネルを作成します。

チャンネルグループの一部である物理ポートに割り当てられたIPアドレスをディセーブルにする必要はありませんが、これをディセーブルにすることを強く推奨します。

interface port-channel コマンドの次に **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ3のポートチャンネルを作成できます。インターフェイスをチャンネルグループに適用する前に、ポートチャンネルの論理インターフェイスを手動で設定してください。

EtherChannel を設定した後、ポートチャンネル インターフェイスに加えられた設定の変更は、そのポートチャンネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャンネル インターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、**spanning-tree** コマンドを使用して、レイヤ2 EtherChannel をトランクとして設定します。

active モードは、ポートをネゴシエーションステートにします。このステートでは、ポートはLACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャンネルは、**active** モードまたは **passive** モードの別のポートグループで形成されます。

auto モードは、ポートをパッシブネゴシエーションステートにします。この場合、ポートは受信する **PAgP** パケットに応答しますが、**PAgP** パケットネゴシエーションを開始することはありません。チャンネルは、**desirable** モードの別のポートグループでだけ形成されます。**auto** がイネーブルの場合、サイレント動作がデフォルトになります。

desirable モードは、ポートをアクティブネゴシエーションステートにします。この場合、ポートは **PAgP** パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、**desirable** モードまたは **auto** モードの別のポートグループで形成されます。**desirable** がイネーブルの場合、サイレント動作がデフォルトになります。

auto モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレントモードを設定するのは、**PAgP** 非対応で、かつほとん

どパケットを送信しない装置にスイッチを接続する場合です。サイレントパートナーの例は、トラフィックを生成しないファイルサーバ、またはパケットアナライザなどです。この場合、物理ポート上で稼働している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャンネルグループにポートを付与したり、伝送用ポートを使用したりできます。リンクの両端はサイレントに設定することはできません。

on モードでは、使用可能な EtherChannel が存在するのは、両方の接続ポートグループが on モードになっている場合だけです。



Caution on モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリーループが発生することがあります。

passive モードは、ポートをネゴシエーションステートにします。この場合、ポートは受信した LACP パケットに応答しますが、LACP パケットネゴシエーションを開始することはありません。チャンネルは、active モードの別のポートグループでだけ形成されます。

EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループは、同一のスイッチ、またはスタックにある異なるスイッチ上で共存できます（クロススタック構成ではできません）。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

channel-protocol インターフェイス コンフィギュレーション コマンドを使用してプロトコルを設定した場合、設定値は、**channel-group** インターフェイス コンフィギュレーション コマンドによっては上書きされません。

アクティブまたはまだアクティブでない EtherChannel メンバとなっているポートを、IEEE 802.1X ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1X 認証をイネーブルにしようとする、エラーメッセージが表示され、IEEE 802.1X 認証はイネーブルになりません。

セキュアポートを EtherChannel の一部として、または EtherChannel ポートをセキュアポートとしては設定しないでください。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。



Caution 物理 EtherChannel ポート上で、レイヤ 3 のアドレスをイネーブルにしないでください。物理 EtherChannel ポート上でブリッジグループを割り当てることは、ループが発生する原因になるため、行わないでください。

次に、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート 2 つを PAgP モード desirable であるチャンネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
```

```
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable
Device(config-if-range)# end
```

次に、スタック内の1つのスイッチに EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセスポート2つを LACP モード active であるチャンネル5に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

次の例では、スイッチスタックのクロススタック EtherChannel を設定する方法を示します。LACP パッシブモードを使用して、VLAN 10 内のスタティックアクセスポートとしてスタックメンバ2のポートを2つ、スタックメンバ3のポートを1つチャンネル5に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/4 - 5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface GigabitEthernet 3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

channel-protocol

ポート上で使用されるプロトコルを制限してチャネリングを管理するには、インターフェイス コンフィギュレーションモードで **channel-protocol** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

channel-protocol {**lACP** | **PAgP**}
no channel-protocol

Syntax Description

lACP Link Aggregation Control Protocol (LACP) で EtherChannel を設定します。

PAgP Port Aggregation Protocol (PAgP) で EtherChannel を設定します。

Command Default

EtherChannel に割り当てられているプロトコルはありません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

channel-protocol コマンドは、チャンネルを LACP または PAgP に制限するためだけに使用します。**channel-protocol** コマンドを使用してプロトコルを設定する場合、設定はインターフェイス コンフィギュレーションモードの **channel-group** コマンドで上書きされることはありません。

インターフェイス コンフィギュレーションモードの **channel-group** コマンドは、EtherChannel のパラメータ設定に使用してください。また、**channel-group** コマンドは、EtherChannel に対しモードを設定することもできます。

EtherChannel グループ上で、PAgP および LACP モードの両方をイネーブルにすることはできません。

PAgP と LACP には互換性がありません。両方ともチャンネルの終端は同じプロトコルを使用する必要があります。

次の例では、EtherChannel を管理するプロトコルとして LACP を指定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# channel-protocol lACP
```

設定を確認するには、特権 EXEC モードで **show etherchannel** [*channel-group-number*] **protocol** コマンドを使用します。

clear l2protocol-tunnel counters

プロトコルトンネルポートのプロトコルカウンタをクリアするには、特権 EXEC モードで **clear l2protocol-tunnel counters** コマンドを使用します。

```
clear l2protocol-tunnel counters [interface-id]
```

Syntax Description	<i>interface-id</i>	(任意) プロトコルカウンタをクリアするインターフェイスまたはポートチャネル。				
Command Default	なし					
Command Modes	特権 EXEC					
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.12.1</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。	
リリース	変更内容					
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。					
Usage Guidelines	スイッチまたは指定されたインターフェイスのプロトコルトンネルカウンタをクリアするには、このコマンドを使用します。					

次の例では、インターフェイスのレイヤ 2 プロトコルトンネルカウンタをクリアする方法を示します。

```
Device# clear l2protocol-tunnel counters gigabitethernet1/0/3
```

clear lacp

Link Aggregation Control Protocol (LACP) チャネルグループカウンタをクリアするには、特権 EXEC モードで **clear lacp** コマンドを使用します。

clear lacp [*channel-group-number*] **counters**

Syntax Description

channel-group-number (任意) チャネルグループ番号。
指定できる範囲は 1 ~ 48 です。

counters トラフィックカウンタをクリアします。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

すべてのカウンタをクリアするには、**clear lacp counters** コマンドを使用します。また、指定のチャネルグループのカウンタのみをクリアするには、**clear lacp channel-group-number counters** コマンドを使用します。

次の例では、すべてのチャネルグループ情報をクリアする方法を示します。

```
Device> enable
Device# clear lacp counters
```

次の例では、グループ 4 の LACP トラフィックのカウンタをクリアする方法を示します。

```
Device> enable
Device# clear lacp 4 counters
```

情報が削除されたことを確認するには、特権 EXEC モードで **show lacp counters** または **show lacp channel-group-number counters** コマンドを入力します。

clear pagp

Port Aggregation Protocol (PAgP) チャンネルグループ情報をクリアするには、特権 EXEC モードで **clear pagp** コマンドを使用します。

clear pagp [*channel-group-number*] **counters**

Syntax Description	<i>channel-group-number</i> (任意) チャンネルグループ番号。 指定できる範囲は 1 ~ 48 です。	
	counters トラフィックカウンタをクリアします。	
Command Modes	特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines すべてのカウンタをクリアするには、**clear pagp counters** コマンドを使用します。また、指定のチャンネルグループのカウンタのみをクリアするには、**clear pagp channel-group-number counters** コマンドを使用します。

次の例では、すべてのチャンネルグループ情報をクリアする方法を示します。

```
Device> enable
Device# clear pagp counters
```

次の例では、グループ 10 の PAgP トラフィックのカウンタをクリアする方法を示します。

```
Device> enable
Device# clear pagp 10 counters
```

情報が削除されたことを確認するには、特権 EXEC モードで **show pagp** コマンドを入力します。

clear spanning-tree counters

スパニングツリーのカウンタをクリアするには、特権 EXEC モードで **clear spanning-tree counters** コマンドを使用します。

clear spanning-tree counters [**interface** *interface-id*]

Syntax Description

interface *interface-id*

(任意) 指定のインターフェイスのスパニングツリーカウンタをクリアします。有効なインターフェイスとしては、物理ポート、VLAN などがあります。

指定できる VLAN 範囲は 1 ~ 4094 です。

指定できるポートチャネルは 1 ~ 48 です。

Command Modes

特権 EXEC

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

interface-id が指定されていない場合は、すべてのインターフェイスのスパニングツリーカウンタがクリアされます。

次の例では、すべてのインターフェイスのスパニングツリーカウンタをクリアする方法を示します。

```
Device> enable
Device# clear spanning-tree counters
```

clear spanning-tree detected-protocols

デバイスでプロトコル移行プロセスを再開して、強制的にネイバーと再ネゴシエーションするには、特権 EXEC モードで **clear spanning-tree detected-protocols** コマンドを使用します。

clear spanning-tree detected-protocols [**interface** *interface-id*]

Syntax Description

interface *interface-id*

(任意) 指定されたインターフェイスでプロトコル移行プロトコル、VLAN、ポートチャネルなどがあります。

指定できる VLAN 範囲は 1 ~ 4094 です。

指定できるポートチャネルは 1 ~ 48 です。

Command Modes

特権 EXEC

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+) プロトコルまたは Multiple Spanning Tree Protocol (MSTP) が稼働するデバイスは、組み込み済みのプロトコル移行方式をサポートしています。それによって、スイッチはレガシー IEEE 802.1D デバイスと相互に動作できるようになります。Rapid PVST+ または MSTP デバイスが、プロトコルのバージョンが 0 に設定されているレガシー IEEE 802.1D コンフィギュレーションブリッジプロトコルデータユニット (BPDU) を受信した場合、そのデバイスはそのポートで IEEE 802.1D BPDU だけを送信します。マルチスパンニングツリー (MST) デバイスが、レガシー BPDU、別のリージョンに対応する MST BPDU (バージョン 3)、または高速スパンニングツリー (RST) BPDU (バージョン 2) を受信したときは、そのポートがリージョンの境界にあることを検知します。

デバイスは、IEEE 802.1D BPDU を受信しなくなった場合であっても、自動的に Rapid PVST+ モードまたは MSTP モードには戻りません。これは、レガシースイッチが指定スイッチでなければ、リンクから削除されたかどうかを学習できないためです。この状況では、**clear spanning-tree detected-protocols** コマンドを使用します。

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

```
Device> enable
```

```
Device# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

debug etherchannel

EtherChannel のデバッグをイネーブルにするには、特権 EXEC モードで **debug etherchannel** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug etherchannel [all | detail | error | event | idb ]
no debug etherchannel [all | detail | error | event | idb ]
```

Syntax Description

all	(任意) EtherChannel デバッグ メッセージをすべて表示します。
detail	(任意) EtherChannel デバッグ メッセージの詳細を表示します。
error	(任意) EtherChannel エラー デバッグ メッセージを表示します。
event	(任意) EtherChannel イベント メッセージを表示します。
idb	(任意) PAgP インターフェイス記述子ブロック デバッグ メッセージを表示します。

Command Default

デバッグはディセーブルです。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

undebug etherchannel コマンドは **no debug etherchannel** コマンドと同じです。



Note **linecard** キーワードは、コマンドラインのヘルプに表示されますが、サポートされていません。

次の例では、すべての EtherChannel デバッグ メッセージを表示する方法を示します。

```
Device> enable
Device# debug etherchannel all
```

次の例では、EtherChannel イベント関連のデバッグ メッセージを表示する方法を示します。

```
Device> enable
Device# debug etherchannel event
```

debug lacp

Link Aggregation Control Protocol (LACP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug lacp** コマンドを使用します。LACP のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug lacp [all | event | fsm | misc | packet]
no debug lacp [all | event | fsm | misc | packet]
```

Syntax Description

all	(任意) LACP デバッグ メッセージをすべて表示します。
event	(任意) LACP イベント デバッグ メッセージを表示します。
fsm	(任意) LACP 有限状態マシン内の変更に関するメッセージを表示します。
misc	(任意) 各種 LACP デバッグ メッセージを表示します。
packet	(任意) 受信および送信 LACP 制御パケットを表示します。

Command Default

デバッグはディセーブルです。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

undebug etherchannel コマンドは **no debug etherchannel** コマンドと同じです。

次の例では、すべての LACP デバッグ メッセージを表示する方法を示します。

```
Device> enable
Device# debug LACP all
```

次の例では、LACP イベントに関連するデバッグ メッセージを表示する方法を示します。

```
Device> enable
Device# debug LACP event
```

debug pagp

Port Aggregation Protocol (PAgP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug pagp** コマンドを使用します。PAgP のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug pagp [all | dual-active | event | fsm | misc | packet]
no debug pagp [all | dual-active | event | fsm | misc | packet]
```

Syntax Description	all	(任意) PAgP デバッグメッセージをすべて表示します。
	dual-active	(任意) デュアルアクティブ検出メッセージを表示します。
	event	(任意) PAgP イベント デバッグ メッセージを表示します。
	fsm	(任意) PAgP 有限状態マシン内の変更に関するメッセージを表示します。
	misc	(任意) 各種 PAgP デバッグ メッセージを表示します。
	packet	(任意) 送受信 PAgP 制御パケットを表示します。

Command Default デバッグはディセーブルです。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **undebug pagp** コマンドは **no debug pagp** コマンドと同じです。

次の例では、すべての PAgP デバッグ メッセージを表示する方法を示します。

```
Device> enable
Device# debug pagp all
```

次の例では、PAgP イベントに関連するデバッグメッセージを表示する方法を示します。

```
Device> enable
Device# debug pagp event
```

debug platform pm

プラットフォーム依存ポートマネージャソフトウェアモジュールのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform pm** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug platform pm {all | counters | errdisable | fec | if-numbers | l2-control | link-status |
platform | pm-vectors [detail] | ses | vlans}
no debug platform pm {all | counters | errdisable | fec | if-numbers | l2-control | link-status
| platform | pm-vectors [detail] | ses | vlans}
```

Syntax Description

all	すべてのポートマネージャデバッグメッセージを表示します。
counters	リモートプロシージャコール (RPC) デバッグメッセージのカウンタを表示します。
errdisable	error-disabled 関連イベントデバッグメッセージを表示します。
fec	転送等価クラス (FEC) プラットフォーム関連イベントデバッグメッセージを表示します。
if-numbers	インターフェイス番号移動イベントデバッグメッセージを表示します。
l2-control	レイヤ 2 制御インフラデバッグメッセージを表示します。
link-status	インターフェイスリンク検出イベントデバッグメッセージを表示します。
platform	ポートマネージャ関数イベントデバッグメッセージを表示します。
pm-vectors	ポートマネージャベクトル関連イベントデバッグメッセージを表示します。
detail	(任意) ベクトル関数の詳細を表示します。
ses	サービス拡張シェルフ (SES) 関連イベントデバッグメッセージを表示します。
vlans	VLAN 作成および削除イベントデバッグメッセージを表示します。

Command Default

デバッグはディセーブルです。

Command Modes 特権 EXEC

Command History		変更内容
	リリース	
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **undebg platform pm** コマンドは **no debug platform pm** コマンドと同じです。

次に、VLAN の作成および削除に関するデバッグ メッセージを表示する例を示します。

```
Device> enable
Device# debug platform pm vlans
```

debug platform udd

プラットフォーム依存の単方向リンク検出 (UDLD) ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform udd** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug platform udd [error | event] [switch switch-number]
no debug platform udd [error | event] [switch switch-number]
```

Syntax Description	error	(任意) エラー条件デバッグ メッセージを表示します。
	event	(任意) UDLD 関連プラットフォームイベントデバッグメッセージを表示します。
	switch switch-number	(任意) 指定されたスタック メンバの UDLD デバッグメッセージを表示します。
Command Default	デバッグはディセーブルです。	
Command Modes	特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

undebg platform udd コマンドは **no debug platform udd** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタックメンバのデバッグをイネーブルにする場合は、特権 EXEC モードで **session switch-number** コマンドを使用してアクティブスイッチからセッションを開始してください。次に、スタック メンバのコマンドラインプロンプトで **debug** コマンドを入力します。

debug spanning-tree

スパニングツリー アクティビティのデバッグをイネーブルにするには、EXEC モードで **debug spanning-tree** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

```
debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions
| general | ha | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events |
exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}
```

Syntax Description

all	スパニングツリーのデバッグ メッセージをすべて表示します。
backbonefast	BackboneFast イベント デバッグ メッセージを表示します。
bpdu	スパニングツリーブリッジプロトコルデータユニット (BPDU) デバッグ メッセージを表示します。
bpdu-opt	最適化された BPDU 処理デバッグ メッセージを表示します。
config	スパニングツリー設定変更デバッグ メッセージを表示します。
etherchannel	EtherChannel サポート デバッグ メッセージを表示します。
events	スパニングツリー トポロジイベント デバッグ メッセージを表示します。
exceptions	スパニングツリー例外デバッグ メッセージを表示します。
general	一般的なスパニングツリー アクティビティ デバッグ メッセージを表示します。
ha	ハイ アベイラビリティ スパニングツリー デバッグ メッセージを表示します。
mstp	Multiple Spanning Tree Protocol (MSTP) イベントをデバッグします。
pvst+	Per VLAN Spanning-Tree Plus (PVST+) イベント デバッグ メッセージを表示します。

root	スパニングツリー ルート イベント デバッグ メッセージを表示します。
snmp	スパニングツリーの Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 処理デバッグ メッセージを表示します。
switch	スイッチ シム コマンド デバッグ メッセージを表示します。このシムは、一般的なスパニングツリー プロトコル (STP) コードと、各デバイスプラットフォーム固有コードとの間のインターフェイスとなるソフトウェアモジュールです。
synchronization	スパニングツリー同期イベント デバッグ メッセージを表示します。
uplinkfast	UplinkFast イベント デバッグ メッセージを表示します。

Command Default デバッグはディセーブルです。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines `undebg spanning-tree` コマンドは `no debug spanning-tree` コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合は、アクティブスイッチでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで `session switch-number` コマンドを使用してアクティブスイッチからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで `debug` コマンドを入力します。

アクティブスイッチで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで `remote command switch-number LINE` コマンドを使用します。

次の例では、すべてのスパニングツリーデバッグメッセージを表示する方法を示します。

```
Device> enable
Device# debug spanning-tree all
```

instance (VLAN)

VLAN または VLAN グループをマルチスパンニングツリー (MST) インスタンスにマッピングするには、MST コンフィギュレーションモードで **instance** コマンドを使用します。デフォルトの内部スパンニングツリー (CIST) インスタンスに VLAN を返すには、このコマンドの **no** 形式を使用します。

instance *instance-id* **vlan** *vlan-range*
no instance *instance-id*

Syntax Description		
	<i>instance-id</i>	指定された VLAN がマップされるインスタンス。有効な範囲は 0 ~ 4094 です。
	vlan <i>vlan-range</i>	指定したインスタンスにマッピングする VLAN の番号を指定します。指定できる範囲は 1 ~ 4094 です。

Command Default VLAN は MST インスタンスにマッピングされません (すべての VLAN は CIST インスタンスにマッピングされます)。

Command Modes MST コンフィギュレーション モード (config-mst)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **vlan** *vlan-range* は、単一の値または範囲として入力されます。マッピングは、絶対的ではなく差分的に行われます。VLAN の範囲を入力した場合には、この範囲が既存のインスタンスに追加されるか、既存のインスタンスから削除されます。マッピングされていない VLAN は、CIST インスタンスにマッピングされます。

Examples

次に、VLAN の範囲を instance 2 にマッピングする例を示します。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 2 vlans 1-100
Device(config-mst)#
```

次に、単一の VLAN を instance 5 にマッピングする例を示します。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 5 vlans 1100
Device(config-mst)#
```

次に、VLAN の範囲を instance 2 から CIST インスタンスに移動する例を示します。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 2 vlans 40-60
Device(config-mst)#
```

次に、instance 2 にマッピングされているすべての VLAN を再び CIST インスタンスに移動する例を示します。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 2
Device(config-mst)#
```

Related Commands

コマンド	説明
name (MST コンフィギュレーションモード)	MST リージョンの名前を設定します。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーションモードを開始します。

interface port-channel

ポートチャンネルにアクセスするか、またはポートチャンネルを作成するには、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用します。ポートチャンネルを削除するには、このコマンドの **no** 形式を使用します。

```
interface port-channel port-channel-number
no interface port-channel
```

Syntax Description

port-channel-number チャンネルグループ番号。

指定できる範囲は1～48です。

Command Default

ポートチャンネル論理インターフェイスは定義されません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

レイヤ 2 EtherChannel では、物理ポートをチャンネルグループに割り当てる前にポートチャンネル インターフェイスを作成する必要はありません。代わりに、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用できます。このコマンドでは、チャンネルグループが最初の物理ポートを獲得すると、ポートチャンネル論理インターフェイスが自動的に作成されます。最初にポートチャンネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャンネルを作成します。

interface port-channel コマンドの次にインターフェイス コンフィギュレーション モードで **no switchport** コマンドを使用して、レイヤ 3 のポートチャンネルを作成できます。インターフェイスをチャンネルグループに適用する前に、ポートチャンネルの論理インターフェイスを手動で設定してください。

チャンネル グループ内の 1 つのポートチャンネルだけが許可されます。



Caution

ポートチャンネル インターフェイスをルーテッドポートとして使用する場合、チャンネルグループに割り当てられた物理ポート上のレイヤ 3 に、アドレスを割り当てないようにしてください。

**Caution**

レイヤ 3 のポートチャネルインターフェイスとして使用されているチャンネルグループの物理ポート上で、ブリッジグループを割り当てることは、ループ発生の原因になるため行わないようにしてください。スパニングツリーもディセーブルにする必要があります。

interface port-channel コマンドを使用するときは、次のガイドラインに従ってください。

- Cisco Discovery Protocol (CDP) を使用する場合には、これを物理ポートで設定してください。ポートチャネルインターフェイスでは設定できません。
- EtherChannel のアクティブメンバであるポートを IEEE 802.1X ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1X をイネーブルにしても、ポートは EtherChannel に加入しません。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーションガイドの「Configuring EtherChannels」の章を参照してください。

次の例では、ポートチャネル番号 5 でポートチャネルインターフェイスを作成する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 5
```

設定を確認するには、特権 EXEC モードで **show running-config** コマンドを入力するか、特権 EXEC モードで **show etherchannel channel-group-number detail** コマンドを入力します。

l2protocol-tunnel

アクセスポート、IEEE 802.1Q トンネルポート、またはポートチャネルでレイヤ2プロトコルのトンネリングをイネーブルにするには、スイッチスタックまたはスタンドアロンスイッチのインターフェイス コンフィギュレーション モードで **l2protocol-tunnel** コマンドを使用します。インターフェイスでトンネリングをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

l2protocol-tunnel [**drop-threshold** | **shutdown-threshold**] [*value*] [**cdp** | **stp** | **vtp**] [**lldp**] [**point-to-point** | [**pagp** | **lacp** | **udld**]]

no l2protocol-tunnel [**drop-threshold** | **shutdown-threshold**] [*value*] [**cdp** | **stp** | **vtp**] [**lldp**] [**point-to-point** | [**pagp** | **lacp** | **udld**]]

Syntax Description

drop-threshold	(任意) インターフェイスがパケットをドロップするまでに受信されるドロップしきい値を、1 秒あたりのレイヤ2プロトコルパケット数の最大レートで設定します。
shutdown-threshold	(任意) インターフェイスがシャットダウンするまでに受信されるシャットダウンしきい値を、1 秒あたりのレイヤ2プロトコルパケット数の最大レートで設定します。
<i>value</i>	インターフェイスがシャットダウンするまでにカプセル化のために受信される1秒あたりのパケット数のしきい値、またはインターフェイスがパケットをドロップするまでのしきい値。指定できる範囲は1～4096です。デフォルトでは、しきい値は設定されていません。
cdp	(任意) CDPのトンネリングをイネーブルにします。または、CDPのシャットダウンしきい値またはドロップしきい値を指定します。
stp	(任意) STPのトンネリングをイネーブルにします。または、STPのシャットダウンしきい値またはドロップしきい値を指定します。
vtp	(任意) VTPのトンネリングをイネーブルにします。または、VTPのシャットダウンしきい値またはドロップしきい値を指定します。
lldp	(任意) LLDPパケットのトンネリングをイネーブルにします。
point-to-point	(任意) PAgP、LACP、およびUDLDパケットのポイントツーポイントトンネリングをイネーブルにします。
pagp	(任意) PAgPのポイントツーポイントトンネリングをイネーブルにします。または、PAgPのシャットダウンしきい値またはドロップしきい値を指定します。
lacp	(任意) LACPのポイントツーポイントトンネリングをイネーブルにします。または、LACPのシャットダウンしきい値またはドロップしきい値を指定します。

udld	(任意) UDLD のポイントツーポイント トンネリングをイネーブルにします。または、UDLD のシャットダウンしきい値またはドロップしきい値を指定します。
-------------	--

Command Default

デフォルトでは、レイヤ 2 プロトコルのトンネリングは設定されていません。

デフォルトでは、レイヤ 2 プロトコル パケット数のシャットダウンしきい値は設定されていません。

デフォルトでは、レイヤ 2 プロトコル パケット数のドロップしきい値は設定されていません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

Usage Guidelines

Cisco Discovery Protocol (CDP)、スパニング ツリー プロトコル (STP)、または VLAN Trunking Protocol (VTP) パケットのトンネリングをイネーブルにできます。また、ポート集約プロトコル (PAgP)、Link Aggregation Control Protocol (LACP)、または単方向リンク検出 (UDLD) パケットのポイントツーポイント トンネリングをイネーブルにできます。

レイヤ 2 パケットをトンネリングするには、このコマンドを入力する必要があります (必要な場合は、プロトコル タイプを指定)。

このコマンドをポート チャネルで入力する場合、チャネル内のすべてのポートが同じ設定になる必要があります。

サービス プロバイダー ネットワーク内のレイヤ 2 プロトコル トンネリングは、レイヤ 2 の情報が確実にネットワーク内のすべてのカスタマー ロケーションに伝播するようにします。プロトコル トンネリングがイネーブルになると、ネットワーク内の伝送用に、プロトコル パケットがシスコの既知のマルチキャスト アドレスでカプセル化されます。パケットが宛先に到着すると、既知の MAC アドレスがレイヤ 2 プロトコル MAC アドレスに置き換えられます。

CDP、STP、および VTP のレイヤ 2 プロトコル トンネリングは、個別にまたは 3 つすべてのプロトコルに対してイネーブルにできます。

サービス プロバイダー ネットワークでは、ポイントツーポイント ネットワーク トポロジをエミュレートして EtherChannel の作成を強化するのに、レイヤ 2 プロトコル トンネルを使用できます。PAgP または LACP のプロトコル トンネリングがサービス プロバイダーのスイッチでイネーブルにされている場合、リモート カスタマー スイッチは、プロトコル データ ユニット (PDU) を受信し、EtherChannel の自動作成をネゴシエートできます。

PAgP、LACP、および UDLD パケットのトンネリングをイネーブルにするには、ポイントツーポイント ネットワーク トポロジが必要になります。リンクダウン検出時間を減らすには、PAgP または LACP パケットのトンネリングをイネーブルにするときにインターフェイスで UDLD もイネーブルにする必要があります。

PAgP、LACP、および UDLD のポイントツーポイント プロトコル トンネリングは、個別にまたは 3 つすべてのプロトコルに対してイネーブルにできます。



Caution PAgP、LACP、および UDLD トンネリングは、ポイントツーポイント トポロジをエミュレートすることだけを目的としています。設定を間違えたことによりトンネリング パケットが多くのポートに送信されると、ネットワーク障害が発生する可能性があります。

shutdown-threshold キーワードを入力して、インターフェイスがシャットダウンするまでにインターフェイスで受信される 1 秒あたりのプロトコルパケット数を制御します。このキーワードにプロトコル オプションが指定されていない場合は、しきい値が各トンネリング レイヤ 2 プロトコルタイプに適用されます。インターフェイスにドロップしきい値も設定する場合は、シャットダウンしきい値がドロップしきい値以上でなければなりません。

シャットダウンしきい値に到達すると、インターフェイスが **errdisable** になります。**errdisable recovery cause l2ptguard** グローバル コンフィギュレーション コマンドを入力してエラーリカバリをイネーブルにした場合、すべての原因がタイムアウトになった時点で、インターフェイスは **error-disabled** ステートからリカバリして動作を再開できるようになります。**l2ptguard** でエラーリカバリ機能をイネーブルにしない場合、インターフェイスは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで **error-disabled** ステートのままになります。

drop-threshold キーワードを入力して、インターフェイスがパケットをドロップするまでにインターフェイスで受信される 1 秒あたりのプロトコルパケット数を制御します。このキーワードにプロトコル オプションが指定されていない場合は、しきい値が各トンネリング レイヤ 2 プロトコルタイプに適用されます。インターフェイスにシャットダウンしきい値も設定する場合は、ドロップしきい値がシャットダウンしきい値以下でなければなりません。

ドロップしきい値に到達すると、受信されるレートがドロップしきい値を下回るまでインターフェイスがレイヤ 2 プロトコルパケットをドロップします。

設定は、NVRAM に保存されます。

レイヤ 2 プロトコル トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

Examples

次の例では、CDP パケットのプロトコル トンネリングをイネーブルにし、シャットダウンしきい値を 50 pps に設定する方法を示します。

```
Device(config-if)# l2protocol-tunnel cdp
Device(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

次の例では、STP パケットのプロトコル トンネリングをイネーブルにし、ドロップしきい値を 400 pps に設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/11
Device(config-if)# l2protocol-tunnel stp
Device(config-if)# l2protocol-tunnel drop-threshold stp 400
```

次の例では、PAgP および UDLD パケットのポイントツーポイントプロトコルトンネリングをイネーブルにし、PAgP ドロップしきい値を 1000 pps に設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport access vlan 19
Device(config-if)# switchport mode dot1q-tunnel
Device(config-if)# l2protocol-tunnel point-to-point pagp
Device(config-if)# l2protocol-tunnel point-to-point udld
Device(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

lacp fast-switchover

Link Aggregation Control Protocol (LACP) 1:1 リンク冗長性を有効にするには、インターフェイス コンフィギュレーション モードで **lacp fast-switchover** コマンドを使用します。LACP 1:1 リンク冗長性を無効にするには、このコマンドの **no** 形式を使用します。

lacp fast-switchover [**dampening** *time*]

no lacp fast-switchover [**dampening** *time*]

Syntax Description	dampening <i>time</i> LACP 1:1 のホットスタンバイダンプニングをイネーブルにします。範囲は 30 ~ 180 秒です。				
Command Default	LACP 1:1 リンク冗長性は、デフォルトで無効になっています。				
Command Modes	インターフェイス コンフィギュレーション (config-if)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.3.1</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。				

Usage Guidelines	<p>lacp fast-switchover コマンドを入力する前に、次の内容を入力する必要があります。</p> <ul style="list-style-type: none"> • ポート チャネル プロトコル タイプは LACP です。 • lacp max-bundle 1 コマンドはポートチャネル上で入力されました。lacp fast-switchover コマンドは、lacp max-bundle コマンドに影響しません。 <p>lacp fast-switchover dampening コマンドを入力する前に、次の内容を入力する必要があります。</p> <ul style="list-style-type: none"> • ポート チャネル プロトコル タイプは LACP です。 • lacp max-bundle 1 コマンドおよび lacp fast-switchover コマンドはポートチャネル上で入力されました。
-------------------------	--

システム プライオリティとポート プライオリティに基づいて LACP 1:1 リンク冗長性を有効にすると、システムプライオリティが高い方のポートは、リンクをアクティブリンクとして選択し、他方のリンクをスタンバイリンクとして選択します (LACP ポートの優先順位が低いほど、プリファレンスは高くなり、LACP システムの優先順位が低いほど、プリファレンスは高くなります)。LACP 1:1 冗長性機能の場合は、アクティブリンクに障害が発生すると、ポートチャネルを停止せずにスタンバイリンクが新しいアクティブリンクとして選択されます。元のアクティブリンクが回復すると、アクティブリンクの状態に戻ります。この変更の際に、ポートチャネルも稼働状態を保ちます。

LACP 1:1 ホットスタンバイダンプニング機能の場合は、アクティブになった後、プライオリティの高いポートへのスイッチオーバーを遅らせるタイマーを設定します。

**Note**

- 最適なパフォーマンスのために、バンドルで設定するポートは2つだけにするようお勧めします（アクティブ1つとホットスタンバイ1つ）。
- LACP EtherChannel の両端で LACP 1:1 冗長性をイネーブルにする必要があります。
- LACP 1:1 冗長性とダンプニングは、LACP ポートチャンネルでのみ動作します。

Examples

次に、LACP 1:1 リンク冗長性を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 40
Device(config-if)# lACP fast-switchover
Device(config-if)# lACP max-bundle 1
```

次に、LACP 1:1 ホットスタンバイ ダンプニングをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 40
Device(config-if)# lACP fast-switchover
Device(config-if)# lACP max-bundle 1
Device(config-if)# lACP fast-switchover dampening 70
```

Related Commands

コマンド	説明
lACP max-bundle	EtherChannel グループに EtherChannel インターフェイスを割り当てて設定します。
show etherchannel	チャンネルの EtherChannel 情報を表示します。
show lACP	LACP チャンネル グループ情報を表示します。

lacp max-bundle

ポートチャンネルで許可されるアクティブ LACP ポートの最大数を定義するには、インターフェイス コンフィギュレーション モードで **lacp max-bundle** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
lacp max-bundle max_bundle_number
no lacp max-bundle
```

Syntax Description	<i>max_bundle_number</i> ポート チャンネルのアクティブ LACP ポートの最大数。指定できる範囲は 1 ~ 8 です。デフォルト値は 8 です。
---------------------------	---

Command Modes	インターフェイス コンフィギュレーション
----------------------	----------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	LACP チャンネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をホットスタンバイ モードにできます。LACP チャンネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にあるデバイスは、ポートプライオリティを使用して、チャンネルにバンドルするポートおよびホットスタンバイモードに置くポートを判別します。他のデバイス（リンクの非制御側終端）上のポートプライオリティは無視されます。
-------------------------	--

lacp max-bundle コマンドには、**port-channel min-links** コマンドで指定される数より大きい数を指定する必要があります。

ホットスタンバイモード（ポートステータスフラグの H で出力に表示）にあるポートを判断するには、特権 EXEC モードで **show etherchannel summary** コマンドを使用します。

次に、ポートチャンネル 2 で最大 5 個のアクティブ LACP ポートを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# lacp max-bundle 5
```

lACP port-priority

Link Aggregation Control Protocol (LACP) のポートプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **lACP port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lACP port-priority *priority*
no lACP port-priority

Syntax Description	<i>priority</i> LACP のポートプライオリティ。指定できる範囲は 1 ～ 65535 です。				
Command Default	デフォルトは 32768 です。				
Command Modes	インターフェイス コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines インターフェイス コンフィギュレーション モードの **lACP port-priority** コマンドは、LACP チャネルグループに 9 つ以上のポートがある場合、バンドルされるポートと、ホットスタンバイモードに置かれるポートを判別します。

LACP チャネルグループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 つのポートを **active** モードに、最大 8 つのポートを **standby** モードにできます。

ポートプライオリティの比較では、数値が小さいほどプライオリティが高くなります。LACP チャネルグループに 9 つ以上のポートがある場合、LACP ポートプライオリティの数値が小さい（つまり、高いプライオリティ値の）8 つのポートがチャネルグループにバンドルされ、それより低いプライオリティのポートはホットスタンバイモードに置かれます。LACP ポートプライオリティが同じポートが 2 つ以上ある場合（たとえば、そのいずれもデフォルト設定の 65535 に設定されている場合）、ポート番号の内部値によりプライオリティが決定されます。



Note LACP リンクを制御するデバイス上にポートがある場合に限り、LACP ポートプライオリティは有効です。リンクを制御するデバイスの判別については、グローバルコンフィギュレーションモードの **lACP system-priority** コマンドを参照してください。

LACP ポートプライオリティおよび内部ポート番号値を表示するには、特権 EXEC モードで **show lACP internal** コマンドを使用します。

物理ポート上での LACP の設定については、このリリースに対応する構成ガイドを参照してください。

次の例では、ポートで LACP ポート プライオリティを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# lACP port-priority 1000
```

設定を確認するには、特権 EXEC モードで **show lACP [channel-group-number] internal** コマンドを使用します。

lacp rate

Link Aggregation Control Protocol (LACP) 制御パケットが LACP がサポートされているインターフェイスに入力されるレートを設定するには、インターフェイスコンフィギュレーションモードで **lacp rate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp rate {normal | fast}
no lacp rate

Syntax Description

normal LACP 制御パケットが通常レート（リンクのバンドル後、30 秒間隔）で入力されるように指定します。

fast LACP 制御パケットが高速レート（1 秒に 1 回）で入力されるように指定します。

Command Default

制御パケットのデフォルトの入力レートは、リンクがバンドルされた後、30 秒間隔です。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

LACP タイムアウトの期間を変更するには、このコマンドを使用します。シスコスイッチの LACP タイムアウト値はインターフェイスで LACP レートの 3 倍に設定されます。**lacp rate** コマンドを使用して、スイッチの LACP タイムアウト値として 90 秒または 3 秒のいずれかを選択できます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

次に、インターフェイス GigabitEthernet 0/0 の高速（1 秒）入力レートを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# lacp rate fast
```

lACP system-priority

Link Aggregation Control Protocol (LACP) のシステムプライオリティを設定するには、デバイスのグローバルコンフィギュレーションモードで **lACP system-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lACP system-priority priority
no lACP system-priority

Syntax Description

priority LACP のシステムプライオリティ。指定できる範囲は 1 ~ 65535 です。

Command Default

デフォルトは 32768 です。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

lACP system-priority コマンドでは、ポートプライオリティを制御する LACP リンクのデバイスが判別されます。

LACP チャネルグループは、同じタイプのイーサネットポートを 16 個まで保有できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。LACP チャネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にあるデバイスは、ポートプライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイモードに置くポートを判別します。他のデバイス（リンクの非制御側終端）上のポートプライオリティは無視されます。

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システムプライオリティの数値が小さい（プライオリティ値の高い）システムが制御システムとなります。どちらのデバイスも同じ LACP システムプライオリティである場合（たとえば、どちらもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（デバイスの MAC アドレス）により制御するデバイスが判別されます。

lACP system-priority コマンドは、デバイス上のすべての LACP EtherChannel に適用されます。

ホットスタンバイモード（ポートステータスフラグの H で出力に表示）にあるポートを判断するには、特権 EXEC モードで **show etherchannel summary** コマンドを使用します。

次の例では、LACP のシステムプライオリティを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# lACP system-priority 20000
```

設定を確認するには、特権 EXEC モードで **show lACP sys-id** コマンドを入力します。

loopdetect

ネットワークループを検出するには、インターフェイスコンフィギュレーションモードで**loopdetect** コマンドを使用します。ループ検出ガードをディセーブルにするには、コマンドの **no** 形式を使用します。

loopdetect [*time* | **action syslog** | **source-port**]
no loopdetect [*time* | **action syslog** | **source-port**]

Syntax Description	<i>time</i>	(任意) ループ検出フレームが送信される時間間隔 (秒単位)。範囲: 0 ~ 10。デフォルトは 5 です。
	action syslog	(任意) ループが検出された場合にシステムメッセージを表示します。
	source-port	(任意) 送信元ポートを errdisable にします。

Command Default ループ検出ガードがイネーブルになっていません。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

Usage Guidelines 要件に応じて、送信元ポートまたは宛先ポートのいずれかを **errdisable** にできます。キーワードまたは変数を指定せずに **loopdetect** コマンドを設定すると、機能が有効になり、ループが検出されたときに宛先ポートが **errdisable** になります。ネットワークとの間のトラフィックフローを適切に制御するため、送信元ポートを **errdisable** に設定することをお勧めします。

loopdetect action syslog コマンドは、システムメッセージのみを表示し、設定されたポートを **errdisable** にしません。**no loopdetect action syslog** コマンドは、システムを最後に設定されたオプションに戻します。

Examples

次に、ループ検出ガードをイネーブルにする例を示します。この例では、宛先ポートはデフォルトで **error-disabled** になっており、ループ検出フレームはデフォルトの 5 秒間隔で送信されます。

```
Device# enable
Device# configure terminal
Device(config)# interface tengigabitethernet 1/0/18
Device(config-if)# loopdetect
```

次に、ループ検出フレームを送信する時間間隔を設定する例を示します。この例では、ループ検出フレームは 7 秒ごとに送信され、宛先ポートはループが検出されると **error-disabled** になります。

```
Device# enable
Device# configure terminal
Device(config)# interface tengigabitethernet 1/0/18
Device(config-if)# loopdetect 7
```

次に、機能をイネーブルにして、システムメッセージのみを表示する例を示します。宛先ポートまたは送信元ポートで実行されるアクションはありません。

```
Device# enable
Device# configure terminal
Device(config)# interface tengigabitethernet 1/0/18
Device(config-if)# loopdetect action syslog
```

次に、機能をイネーブルにし、送信元ポートを error-disable にする例を示します。

```
Device# enable
Device# configure terminal
Device(config)# interface tengigabitethernet 1/0/18
Device(config-if)# loopdetect source-port
```

次の例は、**no loopdetect action syslog** コマンドの動作を示しています。例の最初の部分では、送信元ポートを error-disable にするように機能が設定されています (**loopdetect source-port**)。この機能は、ポートを error-disable にしないようにシステムメッセージを表示するように再設定されます (**loopdetect action syslog**)。この例の最後の部分では、**loopdetect action syslog** コマンドの **no** 形式が設定されています。これにより、システムは最後に設定されたオプションに戻ります。つまり、送信元ポートが error-disable になります。

パート1: 送信元ポートを error-disable にします

```
Device# enable
Device# configure terminal
Device(config)# interface twentyfivegigabitethernet 1/0/20
Device(config-if)# loopdetect source-port
```

パート2: システムメッセージを表示し、ポートを error-disable にしないように再設定します

```
Device(config-if)# loopdetect action syslog
```

パート3: **loopdetect action syslog** の **no** 形式を使用します (Twe1/0/20 を参照)

```
Device(config-if)# no loopdetect action syslog
Device(config-if)# end
```

```
Device# show loopdetect
Interface Interval Elapsed-Time Port-to-Errdisbale ACTION
-----
Twe1/0/1 5 3 errdisable Source Port SYSLOG
Twe1/0/20 5 0 errdisable Source Port ERRDISABLE
Twe2/0/3 5 2 errdisable Dest Port ERRDISABLE
Loopdetect is ENABLED
```

Related Commands

コマンド	説明
show loopdetect	ループ検出ガードがイネーブルになっているすべてのインターフェイスの詳細を表示します。

name (MST)

マルチスパンニングツリー（MST）のリージョン名を設定するには、MST コンフィギュレーションサブモードで **name** コマンドを使用します。デフォルト名に戻すには、このコマンドの **no** 形式を使用します。

name *name*
no name *name*

Syntax Description

name	MST リージョンに付ける名前を指定します。最大 32 文字の任意のstringです。
------	---

Command Modes

MST コンフィギュレーション モード (config-mst)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

同一の VLAN マッピングとコンフィギュレーションバージョン番号を持つ 2 つ以上のデバイスは、領域名が異なると、異なる MST 領域に入っているものと見なされます。



Note **name** コマンドを使用して MST リージョン名を設定する場合には注意してください。間違えると、デバイスが異なる領域に入ってしまいます。設定名は、大文字と小文字が区別されるパラメータです。

Examples

次に、リージョンに名前を付ける例を示します。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# name Cisco
Device(config-mst)#
```

Related Commands

コマンド	説明
instance	VLAN または VLAN セットを MST インスタンスにマッピングします。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。

pagp learn-method

EtherChannel ポートから受信した着信パケットの送信元アドレスを学習するには、インターフェイス コンフィギュレーション モードで **pagp learn-method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
pagp learn-method {aggregation-port | physical-port}
no pagp learn-method
```

Syntax Description

aggregation-port 論理ポート チャンネルでのアドレス ラーニングを指定します。デバイスは、EtherChannel のいずれかのポートを使用して送信元にパケットを送信します。この設定は、デフォルトです。集約ポート ラーニングの場合、どの物理ポートにパケットが届くかは重要ではありません。

physical-port EtherChannel 内の物理ポートでのアドレス ラーニングを指定します。デバイスは、送信元アドレスを学習したのと同じ EtherChannel 内のポートを使用して送信元へパケットを送信します。チャンネルのもう一方の終端では、特定の宛先 MAC または IP アドレスに対してチャンネル内の同じポートが使用されます。

Command Default

デフォルトは、aggregation-port（論理ポート チャンネル）です。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

学習方式は、リンクの両端で同一の設定にする必要があります。

コマンドライン インターフェイス (CLI) で **physical-port** キーワードが指定された場合でも、デバイスがサポートするのは集約ポートでのアドレスラーニングのみです。インターフェイス コンフィギュレーション モードの **pagp learn-method** および **pagp port-priority** コマンドはデバイスのハードウェアには影響を及ぼしませんが、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

デバイスのリンクパートナーが物理ラーナーである場合、インターフェイス コンフィギュレーション モードで **pagp learn-method physical-port** コマンドを使用して物理ポートラーナーとしてデバイスを設定することを推奨します。また、グローバル コンフィギュレーション モードで **port-channel load-balance src-mac** コマンドを使用して、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。インターフェイス コンフィギュレーション モードで **pagp learn-method** コマンドを使用するのは、このような場合のみにしてください。

次の例では、EtherChannel 内の物理ポート上のアドレスを学習するように学習方式を設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# pagp learn-method physical-port
```

次の例では、EtherChannel内のポートチャンネル上のアドレスを学習するように学習方式を設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# pagp learn-method aggregation-port
```

設定を確認するには、特権 EXEC モードで **show running-config** コマンドを入力するか、特権 EXEC モードで **show pagp channel-group-number internal** コマンドを入力します。

pagp port-priority

EtherChannel を経由してすべての Port Aggregation Protocol (PAgP) トラフィックが送信されるポートを選択するには、インターフェイス コンフィギュレーション モードで **pagp port-priority** コマンドを使用します。EtherChannel で使用されていないすべてのポートがホットスタンバイ モードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼働状態にできません。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority *priority*
no pagp port-priority

Syntax Description

priority プライオリティ番号。有効な範囲は0～255です。

Command Default

デフォルト値は 128 です。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

同じ EtherChannel 内で動作可能でメンバーシップを持つ物理ポートの中で最も高いプライオリティを持つポートが、PAgP 送信用として選択されます。

コマンドライン インターフェイス (CLI) で **physical-port** キーワードが指定された場合でも、デバイスがサポートするのは集約ポートでのアドレスラーニングのみです。インターフェイス コンフィギュレーション モードの **pagp learn-method** および **pagp port-priority** コマンドはデバイスのハードウェアには影響を及ぼしませんが、Catalyst 1900 スイッチなど、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

デバイスのリンクパートナーが物理ラーナーである場合、インターフェイス コンフィギュレーション モードで **pagp learn-method physical-port** コマンドを使用して物理ポートラーナーとしてデバイスを設定することを推奨します。また、グローバル コンフィギュレーション モードで **port-channel load-balance src-mac** コマンドを使用して、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。インターフェイス コンフィギュレーション モードで **pagp learn-method** コマンドを使用するのは、このような場合のみにしてください。

次の例では、ポートプライオリティを 200 に設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# pagp port-priority 200
```

設定を確認するには、特権 EXEC モードで **show running-config** コマンドを入力するか、特権 EXEC モードで **show pagp channel-group-number internal** コマンドを入力します。

port-channel

自動作成された EtherChannel を手動チャンネルに変換して、設定を EtherChannel に追加するには、特権 EXEC モードで **port-channel** コマンドを使用します。

port-channel { *channel-group-number* **persistent** | **persistent** }

Syntax Description

channel-group-number チャンネルグループ番号。

指定できる範囲は 1 ~ 48 です。

persistent

自動作成された EtherChannel を手動チャンネルに変更し、EtherChannel への設定の追加を許可します。

Command Modes

特権 EXEC

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

EtherChannel の情報を表示するには、特権 EXEC モードで **show etherchannel summary** コマンドを使用します。

Examples

この例では、自動作成された EtherChannel を手動チャンネルに変換する方法を示します。

```
Device> enable
Device# port-channel 1 persistent
```

port-channel auto

スイッチ上の Auto-LAG 機能をグローバルで有効にするには、グローバル コンフィギュレーション モードで **port-channel auto** コマンドを使用します。スイッチ上の Auto-LAG 機能をグローバルで無効にするには、このコマンドの **no** 形式を使用します。

port-channel auto
no port-channel auto

Command Default

デフォルトでは、Auto-LAG 機能がグローバルで無効にされ、すべてのポート インターフェイスで有効になっています。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

EtherChannel が自動作成されたかどうかを確認するには、特権 EXEC モードで **show etherchannel auto** コマンドを使用します。

Examples

次に、スイッチの Auto-LAG 機能を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# port-channel auto
```

port-channel load-balance

EtherChannel のポート間での負荷分散方式を設定するには、グローバル コンフィギュレーション モードで **port-channel load-balance** コマンドを使用します。ロードバランシング メカニズムをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** | **src-dst-ip** | **src-dst-mac** | **src-dst-mixed-ip-port** | **src-dst-port** | **src-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**}

no port-channel load-balance

Syntax	Description
dst-ip	宛先ホストの IP アドレスに基づいた負荷分散を指定します。
dst-mac	宛先ホストの MAC アドレスに基づいた負荷分散を指定します。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
dst-mixed-ip-port	宛先 IPv4 または IPv6 アドレスと TCP/UDP (レイヤ 4) ポート番号に基づいて負荷分散を指定します。
dst-port	宛先 TCP/UDP (レイヤ 4) と IPv4 と IPv6 の両方のポート番号に基づいて負荷分散を指定します。
extended	EtherChannel のポート間の拡張ロード バランス方式を設定します。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいて負荷分散を指定します。
src-dst-mac	送信元および宛先ホストの MAC アドレスに基づいた負荷分散を指定します。
src-dst-mixed-ip-port	送信元および宛先のホスト IP アドレスと TCP/UDP (レイヤ 4) ポート番号に基づいて負荷分散を指定します。
src-dst-port	送信元および宛先の TCP/UDP (レイヤ 4) ポート番号に基づいて負荷分散を指定します。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散を指定します。
src-mac	送信元の MAC アドレスに基づいた負荷分散を指定します。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-mixed-ip-port	送信元ホスト IP アドレスと TCP/UDP (レイヤ 4) ポート番号に基づいて負荷分散を指定します。
src-port	TCP/UDP (レイヤ 4) ポート番号に基づいて負荷分散を指定します。

Command Default デフォルト値は **src-mac** です。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 設定を確認するには、特権 EXEC モードで **show running-config** コマンドを入力するか、特権 EXEC モードで **show etherchannel load-balance** コマンドを入力します。

Examples

次に、負荷分散方式を dst-mac に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# port-channel load-balance dst-mac
```

Related Commands

コマンド	説明
show etherchannel load-balance	EtherChannel ロードバランシングに関する情報を表示します。
show running-config	実行設定を表示します。

port-channel load-balance extended

EtherChannel のポート間での負荷分散方式の組み合わせを設定するには、グローバルコンフィギュレーション モードで **port-channel load-balance extended** コマンドを使用します。拡張ロードバランシング メカニズムをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
port-channel load-balance extended {dst-ip | dst-mac | dst-port | ipv6-label | l3-proto | src-ip | src-mac | src-port}
no port-channel load-balance extended
```

Syntax Description

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散を指定します。
dst-mac	宛先ホストの MAC アドレスに基づいた負荷分散を指定します。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャンネルの異なるポートに送信されます。
dst-port	宛先 TCP/UDP（レイヤ 4）と IPv4 と IPv6 の両方のポート番号に基づいて負荷分散を指定します。
ipv6-label	送信元 MAC アドレスと IPv6 フロー ラベルに基づいて負荷分散を指定します。
l3-proto	送信元 MAC アドレスとレイヤ 3 プロトコルに基づいて負荷分散を指定します。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散を指定します。
src-mac	送信元の MAC アドレスに基づいた負荷分散を指定します。異なるホストからのパケットは、チャンネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-port	TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。

Command Default

デフォルトは **src-mac** です。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.x	コマンドが変更されました。 port-channel load-balance extended コマンドのキーワードの少なくとも1つを強制的に設定する必要があります。

Usage Guidelines

設定を確認するには、特権 EXEC モードで **show running-config** コマンドを入力するか、特権 EXEC モードで **show etherchannel load-balance** コマンドを入力します。

Examples

次に、拡張負荷分散方式を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip
```

port-channel min-links

ポートチャンネルがアクティブになるように、リンクアップ状態で、EtherChannel にバンドルする必要がある LACP ポートの最小数を定義するには、インターフェイス コンフィギュレーション モードで **port-channel min-links** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel min-links *min_links_number*
no port-channel min-links

Syntax Description

min_links_number ポートチャンネル内のアクティブな LACP ポートの最小数。指定できる範囲は 2 ~ 8 です。デフォルトは 1 です。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

LACP チャンネルグループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をホットスタンバイ モードにできます。LACP チャンネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にあるデバイスは、ポートプライオリティを使用して、チャンネルにバンドルするポートおよびホットスタンバイモードに置くポートを判別します。他のデバイス（リンクの非制御側終端）上のポートプライオリティは無視されます。

port-channel min-links コマンドには、**lacp max-bundle** コマンドで指定される数より小さい数を指定する必要があります。

ホットスタンバイモード（ポートステータスフラグの H で出力に表示）にあるポートを判断するには、特権 EXEC モードで **show etherchannel summary** コマンドを使用します。

次に、ポートチャンネル 2 がアクティブになる前に、少なくとも 3 個のアクティブな LACP ポートを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# port-channel min-links 3
```

rep admin vlan

Resilient Ethernet Protocol (REP) の REP 管理 VLAN を設定して、ハードウェアフラッドレイヤ (HFL) メッセージを送信するには、グローバル コンフィギュレーション モードで **rep admin vlan** コマンドを使用します。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
rep admin vlan vlan-id segment segment-id
no rep admin vlan vlan-id segment segment-id
```

Syntax Description	<i>vlan-id</i>	48 ビット静的 MAC アドレス。
	segment	REP セグメントの管理 VLAN を設定します。
	<i>segment-id</i>	管理 VLAN が割り当てられているセグメントを指定します。セグメント ID 番号の範囲は 1 ~ 1024 です
Command Default	グローバル コンフィギュレーション	
Command Modes	グローバル コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.2.1	segment キーワードが導入されました。

rep block port

Resilient Ethernet Protocol (REP) プライマリエッジポートで REP VLAN ロードバランシングを設定するには、インターフェイス コンフィギュレーション モードで **rep block port** コマンドを使用します。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

rep block port {id *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
no rep block port {id *port-id* | *neighbor-offset* | **preferred**}

Syntax Description

id <i>port-id</i>	REP を有効にすると自動的に生成される一意のポート ID を入力して VLAN ブロック代替ポートを指定します。REP ポート ID は、16 文字の 16 進数値です。
<i>neighbor-offset</i>	ネイバーのオフセット番号を入力することによる、VLAN ブロック代替ポート。範囲は -256 ~ +256 です。値 0 は無効です。
preferred	すでに VLAN ロードバランシングの優先代替ポートとして指定されている通常セグメントポートを選択します。
vlan	ブロックされる VLAN を指定します。
<i>vlan-list</i>	表示される VLAN ID または VLAN ID の範囲。ブロックする VLAN ID (1 ~ 4094 の範囲) を入力するか、ブロックする LAN ID の範囲または連続番号 (1-3、22、41-44 など) を入力します。
all	すべての VLAN をブロックします。

Command Default

特権 EXEC モードで **rep preempt segment** コマンドを入力した後のデフォルト動作では (手動プリエンプレッションの場合)、プライマリエッジポートですべての VLAN をブロックします。この動作は、**rep block port** コマンドを設定するまで継続されます。

プライマリエッジポートで代替ポートを判別できない場合は、デフォルトのアクションはプリエンプレッションなし、および VLAN ロードバランシングなしです。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

オフセット番号を入力して代替ポートを選択する場合、オフセット番号はエッジポートのダウンストリーム ネイバー ポートを識別します。プライマリエッジポートはオフセット番号 1 です。1 を超える正数はプライマリエッジポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリエッジポート (オフセット番号 -1) とダウンストリーム ネイバーを識別します。



Note 番号 1 はプライマリ エッジポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

インターフェイス コンフィギュレーション モードで、**rep preempt delay seconds** コマンドを入力することでプリエンプション遅延時間を設定しており、リンク障害とリカバリが発生した場合、別のリンク障害が発生することなく設定したプリエンプション期間が経過すると、VLAN ロード バランシングが開始されます。ロードバランシング設定で指定された代替ポートは、設定された VLAN をブロックし、その他すべてのセグメントポートのブロックを解除します。プライマリ エッジポートで VLAN バランシングの代替ポートを決定できない場合、デフォルトのアクションはプリエンプションなしになります。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポートのポート ID を判別するには、特権 EXEC モードで **show interfaces interface-id rep detail** コマンドを入力します。

Examples

次に、REP VLAN ロード バランシングを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

Related Commands

コマンド	説明
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep lsl-age-timer

Resilient Ethernet Protocol (REP) リンクステータスレイヤ (LSL) のエージアウトタイマー値を設定するには、インターフェイス コンフィギュレーション モードで **rep lsl-age-timer** コマンドを使用します。デフォルトのエージアウトタイマー値に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-age-timer *milliseconds*
no rep lsl-age-timer *milliseconds*

Syntax Description	<i>milliseconds</i> ミリ秒単位の REP LSL エージアウト タイマー値。範囲は 120 ~ 10000 の 40 の倍数です。
---------------------------	---

Command Default	デフォルトの LSL エージアウト タイマー値は 5 ミリ秒です。
------------------------	-----------------------------------

Command Modes	インターフェイス コンフィギュレーション
----------------------	----------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	REP の設定可能なタイマーを設定する際には、最初に REP LSL の再試行回数を設定し、その後、REP LSL のエージアウト タイマー値を設定することを推奨します。
-------------------------	---

Examples 次に、REP LSL エージアウト タイマー値を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge primary
Device(config-if)# rep lsl-age-timer 2000
```

Related Commands	コマンド	説明
	interface interface-type interface-name	STCNを受信する物理インターフェイスまたはポートチャネルを指定します。
	rep segment	インターフェイス上で REP をイネーブルにし、セグメント ID を割り当てます。

rep lsl-retries

REP リンクステータスレイヤ（LSL）の再試行回数を設定するには、インターフェイス コンフィギュレーション モードで **rep lsl-retries** コマンドを使用します。デフォルトの再試行回数に戻すには、このコマンドの **no** 形式を使用します。

```
rep lsl-retries number-of-retries
no rep lsl-retries number-of-retries
```

Syntax Description	<i>number-of-retries</i> LSL の再試行回数。再試行回数の範囲は、3～10 です。	
Command Default	デフォルトの再試行回数は 5 回です。	
Command Modes	インターフェイス コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Usage Guidelines **rep lsl-retries** コマンドは、REP リンクを無効にする前に再試行回数を設定するために使用されます。REP の設定可能なタイマーを設定する際には、最初に REP LSL の再試行回数を設定し、その後、REP LSL のエージアウト タイマー値を設定することを推奨します。

次に、REP LSL の再試行回数を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 2 edge primary
```

rep preempt delay

セグメントポートの障害およびリカバリの発生後、Resilient Ethernet Protocol (REP) VLAN ロードバランシングがトリガーされるまでの待機時間を設定するには、インターフェイス コンフィギュレーション モードで **rep preempt delay** コマンドを使用します。設定した遅延を削除するには、このコマンドの **no** 形式を使用します。

rep preempt delay seconds
no rep preempt delay

Syntax Description

seconds REP プリエンプションを遅延する秒数です。範囲は 15 ~ 300 秒です。デフォルトは遅延なしの手動プリエンンプションです。

Command Default

REP プリエンプション遅延は設定されていません。デフォルトは遅延なしの手動プリエンンプションです。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

REP プライマリ エッジ ポート上にこのコマンドを入力します。

リンク障害とリカバリ後に自動的に VLAN ロードバランシングをトリガーする場合は、このコマンドを入力してプリエンンプション時間遅延を設定します。

VLAN ロードバランシングが設定されている場合、セグメントポート障害とリカバリの後、VLAN ロードバランシングが発生する前に REP プライマリ エッジポートで遅延タイマーが起動されます。各リンク障害が発生した後にタイマーが再起動することに注意してください。タイマーが満了となると、(インターフェイス コンフィギュレーション モードで **rep block port** コマンドを使用して設定された) VLAN ロードバランシングを実行するように REP プライマリ エッジポートが代替ポートに通知し、新規トポロジ用のセグメントが準備されます。設定された VLAN リストは代替ポートでブロックされ、他のすべての VLAN はプライマリ エッジポートでブロックされません。

設定を確認するには、**show interfaces rep** コマンドを入力します。

Examples

次に、プライマリ エッジポートで REP プリエンプション時間遅延を 100 秒に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep preempt delay 100
```

Related Commands

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep preempt segment

Resilient Ethernet Protocol (REP) VLAN ロードバランシングがセグメントで手動で開始されるようにするには、特権 EXEC モードで **rep preempt segment** コマンドを使用します。

rep preempt segment *segment-id*

Syntax Description

segment-id REP セグメントの ID です。有効な範囲は 1 ~ 1024 です。

Command Default

デフォルト動作は手動プリエンブションです。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デバイスのプライマリ エッジポートがあるセグメントで、次のコマンドを入力します。

VLAN ロードバランシングのプリエンブションを設定する前に、他のすべてのセグメントの設定が完了していることを確認してください。VLAN ロードバランシングのプリエンブションはネットワークを中断する可能性があるため、**rep preempt segment** *segment-id* コマンドを入力すると、このコマンドの実行前に確認メッセージが表示されます。

プライマリエッジポートで、インターフェイス コンフィギュレーション モードから **rep preempt delay** *seconds* コマンドを入力せずに、プリエンブション時間遅延を設定する場合、デフォルト設定はセグメントでの VLAN ロードバランシングの手動トリガーです。

特権 EXEC モードで **show rep topology** コマンドを入力して、セグメント内のどのポートがプライマリエッジポートなのかを確認します。

VLAN ロードバランシングを設定しない場合、**rep preempt segment** *segment-id* コマンドを入力すると、デフォルトの動作が実行されます。つまりプライマリエッジポートがすべての VLAN をブロックします。

REP プライマリエッジポートのインターフェイス コンフィギュレーション モードで **rep block port** コマンドを入力して VLAN ロードバランシングを設定してから、手動でプリエンブションを開始できます。

Examples

次に、セグメント 100 で手動で REP プリエンブションをトリガーする例を示します。

```
Device> enable
Device# rep preempt segment 100
```

Related Commands

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
rep preempt delay	ポート障害とリカバリの後から REP VLAN ロード バランシングがトリガーされるまでの待機期間を設定します。
show rep topology	セグメントまたはすべてのセグメントの REP トポロジ情報を表示します。

rep segment

インターフェイスで Resilient Ethernet Protocol (REP) を有効にし、そのインターフェイスにセグメント ID を割り当てるには、インターフェイス コンフィギュレーションモードで **rep segment** コマンドを使用します。インターフェイスで REP を無効にするには、このコマンドの **no** 形式を使用します。

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]
no rep segment

Syntax Description

segment-id	REP が有効になっているセグメント。セグメント ID をインターフェイスに割り当てます。有効な範囲は 1 ~ 1024 です。
edge	(任意) エッジポートとしてポートを設定します。各セグメントにあるエッジポートは 2 つだけです。
no-neighbor	(任意) セグメント エッジを外部 REP ネイバーなしに指定します。
primary	(任意) プライマリ エッジポート (VLAN ロード バランシングを設定できるポート) としてポートを指定します。1 セグメント内のプライマリ エッジポートは 1 つだけです。
preferred	(任意) ポートを優先代替ポートまたは VLAN ロード バランシングの優先ポートに指定します。 Note ポートを優先ポートに設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。

Command Default

REP はインターフェイスでディセーブルです。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

REP ポートは、レイヤ 2 IEEE 802.1Q ポートまたは 802.1AD ポートのいずれかである必要があります。各 REP セグメント上には、プライマリ エッジポートとセカンダリ エッジポートの 2 種類のエッジポートを設定しなければいけません。

REP がデバイスの 2 つのポートでイネーブルである場合、両方のポートが通常セグメントポートまたはエッジポートのいずれかである必要があります。REP ポートは以下の規則に従います。

- セグメント内のデバイスにポートが1つだけ設定されている場合、そのポートはエッジポートになります。
- 1つのデバイス上で2つのポートが同じセグメントに属する場合、どちらのポートも通常セグメントポートである必要があります。
- 1つのデバイス上で2つのポートが同じセグメントに属し、1つがエッジポートとして設定され、もう1つが通常のセグメントポートとして設定された場合（設定ミス）、エッジポートは通常セグメントポートとして処理されます。



Caution REP インターフェイスはブロック状態で起動し、安全にブロック解除可能と通知されるまでブロック状態のままになります。突然の接続切断を避けるために、これを意識しておく必要があります。

REP がインターフェイスでイネーブルの場合、デフォルトでは通常のセグメントポートであるポートに対してイネーブルになります。

Examples

次に、通常（非エッジ）セグメントポートで REP を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100
```

次に、ポートで REP をイネーブルし、そのポートを REP プライマリ エッジポートとして指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge primary
```

次に、ポートで REP をイネーブルし、そのポートを REP セカンダリ エッジポートとして指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge
```

次に、REP をネイバーなしのエッジポートとして有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge no-neighbor primary
```

rep stcn

セグメントトポロジ変更通知（STCN）を他のインターフェイスまたは他のセグメントに送信するように Resilient Ethernet Protocol（REP）エッジポートを設定するには、インターフェイスコンフィギュレーションモードで **rep stcn** コマンドを使用します。インターフェイスまたはセグメントへの STCN の送信タスクを無効にするには、このコマンドの **no** 形式を使用します。

```
rep stcn {interface interface-id | segment segment-id-list}
no rep stcn {interface | segment}
```

Syntax Description

interface interface-id STCN を受信する物理インターフェイスまたはポート チャンネルを指定します。

segment segment-id-list STCN を受信する 1 つの REP セグメントまたは REP セグメントの一覧を指定します。セグメントの範囲は 1～1024 です。また、一連のセグメント（たとえば 3～5、77、100）を設定することもできます。

Command Default

他のインターフェイスおよびセグメントへの STCN 送信は、無効になっています。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

設定を確認するには、特権 EXEC モードで **show interfaces rep detail** コマンドを入力します。

Examples

次に、セグメント 25～50 に STCN を送信するように REP エッジポートを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep stcn segment 25-50
```

revision

マルチスパンニングツリー（802.1s）（MST）コンフィギュレーションにリビジョン番号を設定するには、MST コンフィギュレーションサブモードで **revision** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

revision *version*
no revision

Syntax Description

version	設定のリビジョン番号を指定します。有効値は 0 ～ 65535 です。
---------	-------------------------------------

Command Default

version : 0

Command Modes

MST コンフィギュレーション モード（config-mst）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

設定が同じでも、リビジョン番号が異なるデバイスは、2つの異なるリージョンに属していると見なされます。



Note MST コンフィギュレーションのリビジョン番号を設定するのに **revision** コマンドを使用する場合には注意が必要です。設定を間違えると、スイッチは異なったリージョンに置かれる可能性があります。

Examples

次に、MSTコンフィギュレーションのリビジョン番号を設定する例を示します。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# revision 5
Device(config-mst)#
```

Related Commands

コマンド	説明
instance	VLAN または VLAN セットを MST インスタンスにマッピングします。
name （MST コンフィギュレーションサブモード）	MST リージョンの名前を設定します。
show spanning-tree	スパンニングツリーステートに関する情報を表示します。

コマンド	説明
spanning-tree mst configuration	MST コンフィギュレーションサブモードを開始します。

show dot1q-tunnel

IEEE 802.1Q トンネルポートに関する情報を表示するには、EXEC モードで **show dot1q-tunnel** コマンドを使用します。

```
show dot1q-tunnel [interface interface-id]
```

Syntax Description	interface interface-id (任意) IEEE 802.1Q トンネリング情報を表示するインターフェイスを指定します。有効なインターフェイスには、物理ポートとポートチャンネルが含まれます。				
Command Default	なし				
Command Modes	ユーザ EXEC 特権 EXEC				
Command History	<table border="1"><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.12.1</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。				

Examples

次の例では、**show dot1q-tunnel** コマンドの出力を示します。

```
Device# show dot1q-tunnel
```

```
dot1q-tunnel mode LAN Port(s)
-----
Gi1/0/1
Gi1/0/2
Gi1/0/3
Gi1/0/6
Po2
```

```
Device# show dot1q-tunnel interface gigabitethernet1/0/1
```

```
dot1q-tunnel mode LAN Port(s)
-----
Gi1/0/1
```

show etherchannel

チャンネルの EtherChannel 情報を表示するには、ユーザ EXEC モードで **show etherchannel** コマンドを使用します。

show etherchannel [*channel-group-number* | {**detail** | **port** | **port-channel** | **protocol** | **summary**}] | [**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**]

Syntax Description	
<i>channel-group-number</i>	(任意) チャンネルグループ番号。 指定できる範囲は 1 ~ 48 です。
detail	(任意) 詳細な EtherChannel 情報を表示します。
load-balance	(任意) ポートチャンネル内のポート間の負荷分散方式、またはフレーム配布方式を表示します。
port	(任意) EtherChannel ポートの情報を表示します。
port-channel	(任意) ポートチャンネル情報を表示します。
protocol	(任意) EtherChannel で使用されるプロトコルを表示します。
summary	(任意) 各チャンネルグループのサマリーを 1 行で表示します。

Command Modes ユーザ EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines チャンネルグループ番号を指定しない場合は、すべてのチャンネルグループが表示されます。出力では、パッシブポートリストフィールドはレイヤ3のポートチャンネルだけで表示されます。このフィールドは、まだ起動していない物理ポートがチャンネルグループ内で設定されていること（および間接的にチャンネルグループ内で唯一のポートチャンネルであること）を意味します。

次に、**show etherchannel channel-group-number detail** コマンドの出力例を示します。

```
Device> show etherchannel 1 detail
Group state = L2
Ports: 2    Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:    LACP
              Ports in the group:
              -----
```

```

Port: Gi1/0/1
-----
Port state      = Up Mstr In-Bndl
Channel group  = 1          Mode = Active          Gcchange = -
Port-channel   =          PoIGC = -          Pseudo port-channel = Po1
Port index     =          0Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
      A - Device is in active mode.          P - Device is in passive mode.

Local information:

Port      Flags  State  LACP port  Admin  Oper  Port  Port
          SA    bndl   Priority   Key    Key   Number State
Gi1/0/1  SA    bndl   32768     0x1    0x1   0x101 0x3D
Gi1/0/2  A     bndl   32768     0x0    0x1   0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

          Port-channels in the group:
          -----

Port-channel: Po1 (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----
0      00    Gi1/0/1   Active        0
0      00    Gi1/0/2   Active        0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2

```

次に、**show etherchannel channel-group-number summary** コマンドの出力例を示します。

```

Device> show etherchannel 1 summary
Flags: D - down P - in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      u - unsuitable for bundling
      U - in use f - failed to allocate aggregator
      d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SU)        LACP      Gi1/0/1(P) Gi1/0/2(P)

```

次に、**show etherchannel channel-group-number port-channel** コマンドの出力例を示します。

```

Device> show etherchannel 1 port-channel
Port-channels in the group:
-----

```

```
Port-channel: Po1 (Primary Aggregator)
-----
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load  Port    EC state          No of bits
-----+-----+-----+-----+-----
  0      00    Gi1/0/1 Active          0
  0      00    Gi1/0/2 Active          0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

次に、**show etherchannel protocol** コマンドの出力例を示します。

```
Device# show etherchannel protocol
Channel-group listing:
-----
Group: 1
-----
Protocol: LACP
Group: 2
-----
Protocol: PAgP
```

show interfaces rep detail

管理 VLAN を含む、すべてのインターフェイスまたは指定されたインターフェイスの詳細な Resilient Ethernet Protocol (REP) の設定およびステータスを表示するには、特権 EXEC モードで **show interfaces rep detail** コマンドを使用します。

show interfaces [*interface-id*] **rep detail**

Syntax Description	<i>interface-id</i> (任意) ポート ID を表示するために使用される物理インターフェイス。	
Command Modes	特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、1 つ以上のセグメントまたは 1 つのインターフェイスに STCN を送信先するために、セグメント エッジ ポートで入力します。

設定を確認するには、特権 EXEC モードで **show interfaces rep detail** コマンドを入力します。

Examples

次に、指定されたインターフェイスに関する REP 設定とステータスを表示する例を示します。

```
Device> enable
Device# show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

Related Commands

コマンド	説明
rep admin vlan	REP が HFL メッセージを送信するための REP 管理 VLAN を設定します。

show l2protocol-tunnel

レイヤ 2 プロトコルトンネルポートに関する情報を表示するには、EXEC モードで **show l2protocol-tunnel** コマンドを使用します。

show l2protocol-tunnel [interface interface-id] summary

Syntax Description	interface interface-id (任意) プロトコルトンネリング情報を表示するインターフェイスを指定します。有効なインターフェイスは物理ポートとポートチャンネルです。指定できるポートチャンネルの範囲は 1 ~ 48 です。
	summary (任意) レイヤ 2 プロトコル サマリー情報だけを表示します。

Command Default なし

Command Modes ユーザ EXEC
特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

Usage Guidelines **l2protocol-tunnel** インターフェイス コンフィギュレーション コマンドを使用してアクセスまたは IEEE 802.1Q トンネルポートのレイヤ 2 プロトコルトンネリングをイネーブルにした後、次のパラメータの一部またはすべてを設定できます。

- トンネリングするプロトコル タイプ
- シャットダウンしきい値
- ドロップしきい値

show l2protocol-tunnel interface コマンドを入力すると、すべてのパラメータが設定されたアクティブポートに関する情報だけが表示されます。

show l2protocol-tunnel summary コマンドを入力すると、一部またはすべてのパラメータが設定されたアクティブポートに関する情報だけが表示されます。

Examples

次に、**show l2protocol-tunnel** コマンドの出力例を示します。

```
Device> show l2protocol-tunnel

COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port          Protocol Shutdown Drop      Encapsulation Decapsulation Drop
              Threshold Threshold Counter      Counter      Counter
-----
-----
```

show l2protocol-tunnel

```

Gi3/0/3  ---      ----      ----      ----      ----      ----
          ---      ----      ----      ----      ----      ----
          pagp    ----      ----      0          242500
          lacp    ----      ----      24268      242640
          udld    ----      ----      0          897960
Gi3/0/4  ---      ----      ----      ----      ----      ----
          ---      ----      ----      ----      ----      ----
          pagp    1000     ----      24249      242700
          lacp    ----      ----      24256      242660
          udld    ----      ----      0          897960
Gi6/0/1  cdp      ----      ----      134482     1344820
          ---      ----      ----      ----      ----      ----
          pagp    1000     ----      0          242500
          lacp    500      ----      0          485320
          udld    300      ----      44899      448980
Gi6/0/2  cdp      ----      ----      134482     1344820
          ---      ----      ----      ----      ----      ----
          pagp    ----      1000     0          242700
          lacp    ----      ----      0          485220
          udld    300      ----      44899      448980

```

次に、**show l2protocol-tunnel summary** コマンドの出力例を示します。

```
Device> show l2protocol-tunnel summary
```

```
COS for Encapsulated Packets: 5
```

```
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Drop Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Status
Gi3/0/2	pagp lacp udld	----/----/----	----/----/----	up
Gi4/0/3	pagp lacp udld	1000/ 500/----	----/----/----	up
Gi9/0/1	pagp ---- ----	----/----/----	1000/----/----	down
Gi9/0/2	pagp ---- ----	----/----/----	1000/----/----	down

show lacp

Link Aggregation Control Protocol (LACP) チャンネルグループ情報を表示するには、ユーザ EXEC モードで **show lacp** コマンドを使用します。

```
show lacp [channel-group-number] {counters | internal | neighbor | sys-id}
```

Syntax Description	
<i>channel-group-number</i>	(任意) チャンネルグループ番号。 指定できる範囲は 1 ~ 48 です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。
sys-id	LACPによって使用されるシステム識別子を表示します。システム識別子は、LACP システムプライオリティとデバイス MAC アドレスで構成されています。

Command Modes ユーザ EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show lacp** コマンドを入力すると、アクティブなチャンネルグループの情報が表示されます。特定のチャンネル情報を表示するには、チャンネルグループ番号を指定して **show lacp** コマンドを入力します。

チャンネルグループを指定しない場合は、すべてのチャンネルグループが表示されます。

channel-group-number を入力すると、**sys-id** 以外のすべてのキーワードでチャンネルグループを指定できます。

次の例では、**show lacp counters** ユーザ EXEC コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show lacp counters
          LACPDUs      Marker      Marker Response      LACPDUs
Port      Sent  Recv      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group:1
Gi2/0/1   19   10         0    0         0    0         0
Gi2/0/2   14    6         0    0         0    0         0
```

Table 98: show lacp counters のフィールドの説明

フィールド	説明
LACPDU Sent および Recv	ポートによって送受信された LACP パケット数
Marker Sent および Recv	ポートによって送受信された LACP Marker パケット数
Marker Response Sent および Recv	ポートによって送受信された LACP Marker 応答パケット数
LACPDU Pkts および Err	ポートの LACP によって受信された、未知で不正なパケット数

次に、**show lacp internal** コマンドの出力例を示します。

```
Device> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode           P - Device is in Passive mode

Channel group 1
Port      Flags  State      LACP port  Admin  Oper  Port  Port
          SA   bndl      Priority   Key    Key   Number State
Gi2/0/1   SA   bndl      32768     0x3    0x3   0x4   0x3D
Gi2/0/2   SA   bndl      32768     0x3    0x3   0x5   0x3D
```

次の表に、出力されるフィールドの説明を示します。

Table 99: show lacp internal のフィールドの説明

フィールド	説明
State	<p>特定のポートの状態。次に使用可能な値を示します。</p> <ul style="list-style-type: none"> • -: ポートの状態は不明です。 • bndl: ポートがアグリゲータに接続され、他のポートとバンドルされています。 • susp: ポートが中断されている状態で、アグリゲータには接続されていません。 • hot-sby: ポートがホットスタンバイの状態です。 • indiv: ポートは他のポートとバンドルできません。 • indep: ポートは独立状態です。バンドルされていませんが、データトラフィックを処理することができます。この場合、LACP は相手側ポートで実行されていません。 • down: ポートがダウンしています。
LACP Port Priority	<p>ポートのプライオリティ設定。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、LACP はポートプライオリティを使用してポートをスタンバイモードにします。</p>
Admin Key	<p>ポートに割り当てられた管理用のキー。LACP は自動的に管理用のキー値を生成します（16進数）。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。ポートが他のポートと集約できるかどうかは、ポートの物理特性（たとえば、データレートやデュプレックス機能）と設定に指定された制限によって決定されます。</p>
Oper Key	<p>ポートで使用される実行時の操作キー。LACP は自動的に値を生成します（16進数）。</p>
Port Number	<p>ポート番号。</p>

フィールド	説明
Port State	<p>ポートの状態変数。1つのオクテット内で個々のビットとしてエンコードされ、次のような意味になります。</p> <ul style="list-style-type: none"> • bit0: LACP のアクティビティ • bit1: LACP のタイムアウト • bit2: 集約 • bit3: 同期 • bit4: 収集 • bit5: 配信 • bit6: デフォルト • bit7: 期限切れ <p>Note 上のリストでは、bit7 が MSB で bit0 は LSB です。</p>

次に、**show lacp neighbor** コマンドの出力例を示します。

```
Device> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs   F - Device is sending Fast LACPDUs
       A - Device is in Active mode          P - Device is in Passive mode
```

Channel group 3 neighbors

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/1	32768,0007.eb49.5e80	0xC	19s	SP
	LACP Partner	Partner	Partner	
	Port Priority	Oper Key	Port State	
	32768	0x3	0x3C	

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/2	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner	Partner	Partner	
	Port Priority	Oper Key	Port State	
	32768	0x3	0x3C	

次に、**show lacp sys-id** コマンドの出力例を示します。

```
Device> show lacp sys-id
32765,0002.4b29.3a00
```

システム ID は、システム プライオリティおよびシステム MAC アドレスで構成されています。最初の 2 バイトはシステム プライオリティ、最後の 6 バイトはグローバルに管理されているシステム関連の個々の MAC アドレスです。

show loopdetect

ループ検出ガードがイネーブルになっているすべてのインターフェイスの詳細を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show loopdetect** コマンドを使用します。

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

Examples

次に、**show loopdetect** コマンドの出力例を示します。

```
Device# show loopdetect
Interface Interval Elapsed-Time Port-to-Errdisbale ACTION
-----
Twe1/0/1      5          3      errdisable Source Port  SYSLOG
Twe1/0/20     5          0      errdisable Source Port  ERRDISABLE
Twe2/0/3      5          2      errdisable Dest Port    ERRDISABLE
Loopdetect is ENABLED
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 100: show loopdetect のフィールドの説明

フィールド	説明
Interface	ループ検出ガードがイネーブルになっているインターフェイスを表示します。
Interval	ループ検出フレームを送信する間隔の設定を、秒単位で表示します。
Elapsed-Time	ループ検出フレームを送信する間隔の設定内で、経過した時間を表示します。
Port-to-Errdisbale	error-disabled に設定されているポートを表示します。
Action	ネットワークループを検出したときにシステムが実行するアクションを表示します。

show pagp

ポート集約プロトコル (PAgP) のチャンネルグループ情報を表示するには、EXEC モードで **show pagp** コマンドを使用します。

```
show pagp [channel-group-number] {counters | dual-active | internal | neighbor}
```

Syntax Description

channel-group-number (任意) チャンネルグループ番号。

指定できる範囲は 1 ~ 48 です。

counters トラフィック情報を表示します。

dual-active デュアルアクティブステータスが表示されます。

internal 内部情報を表示します。

neighbor ネイバーの情報を表示します。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show pagp コマンドを入力すると、アクティブなチャンネルグループの情報が表示されます。非アクティブポートチャンネルの情報を表示するには、チャンネルグループ番号を指定して **show pagp** コマンドを入力します。

Examples

次に、**show pagp 1 counters** コマンドの出力例を示します。

```
Device> show pagp 1 counters
          Information          Flush
Port      Sent  Recv      Sent  Recv
-----
Channel group: 1
  Gi1/0/1   45   42         0     0
  Gi1/0/2   45   41         0     0
```

次に、**show pagp dual-active** コマンドの出力例を示します。

```
Device> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
Port      Dual-Active   Partner      Partner   Partner
          Detect Capable Name          Port      Version
```

```

Gi1/0/1  No          -p2          Gi3/0/3  N/A
Gi1/0/2  No          -p2          Gi3/0/4  N/A

```

<output truncated>

次に、**show pagp 1 internal** コマンドの出力例を示します。

```

Device> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

```

```

Channel group 1

```

Port	Flags	State	Timers	Hello Interval	Partner Count	PAGP Priority	Learning Method	Group Ifindex
Gi1/0/1	SC	U6/S7	H	30s	1	128	Any	16
Gi1/0/2	SC	U6/S7	H	30s	1	128	Any	16

次に、**show pagp 1 neighbor** コマンドの出力例を示します。

```

Device> show pagp 1 neighbor
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

```

```

Channel group 1 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Partner Flags	Partner Group Cap.
Gi1/0/1	-p2	0002.4b29.4600	Gi01//1	9s	SC	10001
Gi1/0/2	-p2	0002.4b29.4600	Gi1/0/2	24s	SC	10001

show platform etherchannel

プラットフォーム依存 EtherChannel 情報を表示するには、特権 EXEC モードで **show platform etherchannel** コマンドを使用します。

```
show platform etherchannel channel-group-number {group-mask | load-balance mac src-mac
dst-mac [ip src-ip dst-ip [port src-port dst-port]]} [switch switch-number]
```

Syntax Description

<i>channel-group-number</i>	チャンネルグループ番号。 指定できる範囲は 1 ~ 48 です。
group-mask	EtherChannel グループ マスクを表示します。
load-balance	EtherChannel ロード バランシングのハッシュ アルゴリズムをテストします。
mac <i>src-mac</i> <i>dst-mac</i>	送信元と宛先の MAC アドレスを指定します。
ip <i>src-ip</i> <i>dst-ip</i>	(任意) 送信元と宛先の IP アドレスを指定します。
port <i>src-port</i> <i>dst-port</i>	(任意) 送信元と宛先のレイヤ ポート番号を指定します。
switch <i>switch-number</i>	(任意) スタック メンバを指定します。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、テクニカル サポート 担当者とともに問題解決を行う場合にだけ使用してください。

テクニカル サポート 担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform pm

プラットフォーム依存のポートマネージャ情報を表示するには、特権 EXEC モードで **show platform pm** コマンドを使用します。

```
show platform pm {etherchannel channel-group-number group-mask | interface-numbers | port-data interface-id | port-state}
```

Syntax Description	
etherchannel <i>channel-group-number</i> group-mask	指定されたチャンネルグループの EtherChannel グループ マスク テーブルを表示します。 指定できる範囲は 1 ~ 48 です。
interface-numbers	インターフェイス番号情報を表示します。
port-data <i>interface-id</i>	指定されたインターフェイスのポート データ情報を表示します。
port-state	ポートの状態情報を表示します。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。
テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show rep topology

セグメント、またはセグメント内のプライマリおよびセカンダリエッジポートを含むすべてのセグメントの Resilient Ethernet Protocol (REP) トポロジ情報を表示するには、特権 EXEC モードで **show rep topology** コマンドを使用します。

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

Syntax Description	segment <i>segment-id</i>	(任意) REP トポロジ情報を表示するセグメントを指定します。セグメント ID の範囲は 1 ~ 1024 です。
	archive	(任意) セグメントの前のトポロジを表示します。このキーワードは、リンク障害のトラブルシューティングに役立ちます。
	detail	(任意) REP トポロジの詳細情報を表示します。
Command Modes	特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**show rep topology** コマンドの出力例を示します。

```
Device# show rep topology

REP Segment 1
BridgeName      PortName      Edge Role
-----
10.64.106.63    Te5/4         Pri  Open
10.64.106.228   Te3/4         Open
10.64.106.228   Te3/3         Open
10.64.106.67    Te4/3         Open
10.64.106.67    Te4/4         Alt
10.64.106.63    Te4/4         Sec  Open

REP Segment 3
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi50/1        Pri  Open
SVT_3400_2      Gi0/3         Open
SVT_3400_2      Gi0/4         Open
10.64.106.68    Gi40/2        Open
10.64.106.68    Gi40/1        Open
10.64.106.63    Gi50/2        Sec  Alt
```

次に、**show rep topology detail** コマンドの出力例を示します。

```
Device# show rep topology detail

REP Segment 1
10.64.106.63, Te5/4 (Primary Edge)
```

```
Open Port, all vlans forwarding
Bridge MAC: 0005.9b2e.1700
Port Number: 010
Port Priority: 000
Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0005.9b1b.1f20
Port Number: 010
Port Priority: 000
Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0005.9b1b.1f20
Port Number: 00E
Port Priority: 000
Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0005.9b2e.1800
Port Number: 008
Port Priority: 000
Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
Alternate Port, some vlans blocked
Bridge MAC: 0005.9b2e.1800
Port Number: 00A
Port Priority: 000
Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
Open Port, all vlans forwarding
Bridge MAC: 0005.9b2e.1700
Port Number: 00A
Port Priority: 000
Neighbor Number: 6 / [-1]
```

show spanning-tree

指定されたスパニングツリー インスタンスのスパニングツリー情報を表示するには、特権 EXEC モードで **show spanning-tree** コマンドを使用します。

show spanning-tree [*bridge-group*] [**active** | **backbonefast** | **blockedports** | **bridge** [*id*] | **detail** | **inconsistentports** | **instances** | **interface** *interface-type interface-number* | **mst** [*list*] | **configuration** [**digest**]] | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*]

Syntax Description	
<i>bridge-group</i>	(任意) ブリッジグループ番号を指定します。指定できる範囲は1～255です。
active	(任意) アクティブインターフェイスに関するスパニングツリー情報だけを表示します。
backbonefast	(任意) スパニングツリー BackboneFast ステータスを表示します。
blockedports	(任意) ブロックされたポート情報を表示します。
bridge	(任意) このスイッチのステータスおよび設定を表示します。
detail	(任意) ステータスおよび設定の詳細を表示します。
inconsistentports	(任意) 不整合ポートに関する情報を表示します。
instances	(任意) 最大 STP インスタンスに関する情報を表示します。
interface <i>interface-type interface-number</i>	(任意) インターフェイスのタイプおよび番号を指定します。各インターフェイス識別子は、前後のものとの区切りを示すためにスペースを使用して入力します。インターフェイスの範囲は入力できません。有効なインターフェイスには、物理ポートおよび仮想 LAN (VLAN) があります。有効な値については、「使用上のガイドライン」を参照してください。
mst	(任意) 複数のスパニングツリーを指定します。
<i>list</i>	(任意) 複数のスパニングツリー インスタンスのリストを指定します。
configuration digest	(任意) マルチスパニングツリーの現在のリージョン設定を表示します。
pathcost method	(任意) 使用されているデフォルトパスコスト計算方式を表示します。有効な値については、「使用上のガイドライン」セクションを参照してください。
root	(任意) ルートスイッチのステータスおよび設定を表示します。

summary	(任意) ポート ステートのサマリーを指定します。
totals	(任意) スパニングツリー ステート セクションのすべての行を表示します。
uplinkfast	(任意) スパニングツリー UplinkFast ステータスを表示します。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。指定できる範囲は 1 ~ 4094 です。 <i>vlan-id</i> の値を省略すると、このコマンドはすべての VLAN のスパニングツリー インスタンスに適用されます。
id	(任意) スパニングツリー ブリッジを識別します。
port-channel <i>number</i>	(任意) インターフェイスに関連付けられたイーサネットチャンネルを識別します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show spanning-tree コマンドで使用できるキーワードおよび引数は、ご使用のプラットフォームおよび設置されて動作可能なネットワークモジュールによって異なります。

257 ~ 282 の **port-channel number** 値は、コンテンツスイッチングモジュール (CSM) およびファイアウォール サービス モジュール (FWSM) でのみサポートされています。

interface-number 引数では、モジュールおよびポート番号を指定します。*interface-number* の有効な値は、指定するインターフェイスタイプと、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビットイーサネットインターフェイスを指定すると、モジュール番号の有効値は 2 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

多数の VLAN が存在し、スパニングツリーのアクティブステートをチェックする場合は、**show spanning-tree summary total** コマンドを入力します。VLAN のリストをスクロールしなくても VLAN の総数を表示できます。

キーワード **pathcoast method** の有効値は次のとおりです。

- **append:** (アペンド動作をサポートしている) URL にリダイレクト出力をアペンドします。
- **begin:** 一致した行から開始します。
- **exclude:** 一致した行を除外します。
- **include:** 一致した行を含みます。
- **redirect:** URL に出力をリダイレクトします。

- **tec:** URL に出力をコピーします。

VLAN またはインターフェイスに対して **show spanning-tree** コマンドを実行すると、スイッチルータは VLAN またはインターフェイスのさまざまなポートステータスを表示します。スパンニングツリーの有効なポートステータスは、**learning**、**forwarding**、**blocking**、**disabled**、および **loopback** です。

```
Device#
show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
            Address    5c71.0dfe.8380
            This bridge is the root
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
            Address    5c71.0dfe.8380
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

Interface          Role Sts Cost      Prio.Nbr Type
-----
Gi1/0/1            Desg FWD 20000    128.1   P2p
Gi1/0/18           Desg FWD 20000    128.18  P2p
Gi1/0/21           Desg FWD 20000    128.21  P2p
Tel/0/25           Desg FWD 20000    128.25  P2p
Tel/0/37           Desg FWD 2000    128.37  P2p
Tel/0/38           Desg FWD 2000    128.38  P2p
Tel/0/45           Desg FWD 20000    128.45  P2p
Tel/0/48           Desg FWD 20000    128.48  P2p
```

ポートステータスの定義については、以下の表を参照してください。

Table 101: show spanning-tree vlan コマンドのポートステータス

フィールド	定義
BLK	ブロック: ポートが BPDU パケットを送信およびリッスンしているが、トラフィックを転送していない。
DIS	無効: ポートが BPDU パケットを送信およびリッスンしておらず、トラフィックを転送していない。
FWD	転送: ポートが BPDU パケットを送信およびリッスンし、トラフィックを転送している。
LBK	ループバック: ポートが自身の BPDU パケットを再受信する。
LIS	リスニング: ポートスパンニングツリーが最初にルートブリッジ用の BPDU パケットのリスニングを開始する。
LRN	ラーニング: ポートが BPDU パケットのプロポーザルビットを設定し、送信する。

次の例では、インターフェイス情報のサマリーを表示する方法を示します。

show spanning-tree

```

Device#
show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
            Address    6cb2.ae4a.4fc0
            This bridge is the root
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address    6cb2.ae4a.4fc0
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

```

```

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fif1/0/17          Desg FWD 2000     128.17  P2p
Fif1/0/19          Desg FWD 800     128.19  P2p
Fif1/0/21          Desg FWD 2000     128.21  P2p
Fif1/0/23          Desg FWD 2000     128.23  P2p
TwoH1/0/42         Desg FWD 500     128.42  P2p
Fou1/0/44          Desg FWD 50     128.44  P2p
Fif2/0/17          Back BLK 2000     128.185 P2p
Fif2/0/19          Back BLK 800     128.187 P2p
Fif2/0/21          Back BLK 2000     128.189 P2p
Fif2/0/23          Back BLK 2000     128.191 P2p
Fou2/0/43          Desg FWD 50     128.211 P2p
Fou2/0/44          Back BLK 50     128.212 P2p
Hu5/0/13           Desg FWD 500     128.685 P2p
Hu5/0/15           Desg FWD 500     128.687 P2p
Hu5/0/21           Back BLK 500     128.693 P2p
Hu5/0/23           Back BLK 500     128.695 P2p
Fou6/0/27          Back BLK 50     128.867 P2p
Hu6/0/29           Desg FWD 200     128.869 P2p
Hu6/0/30           Back BLK 200     128.870 P2p

```

次の表に、この例で表示されるフィールドについて説明します。

Table 102: show spanning-tree コマンド出力のフィールド

フィールド	定義
Port ID Prio.Nbr	ポート ID およびプライオリティ番号
Cost	ポート コスト
Sts	ステータス情報。

次に、現在のブリッジのスパニングツリー情報だけを表示する例を示します。

```

Device# show spanning-tree bridge

Vlan          Bridge ID          Hello Time  Max Age  Fwd Dly  Protocol
-----
VLAN0001      32769 (32768, 1) 5c71.0dfe.8380  2       20    15    rstp

```

次に、インターフェイスに関する詳細情報を表示する例を示します。

```

Device#
show spanning-tree detail
VLAN0001 is executing the rstp compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 5c71.0dfe.8380
Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 27 last change occurred 4d19h ago
    from TenGigabitEthernet1/0/48
Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (GigabitEthernet1/0/1) of VLAN0001 is designated forwarding
  Port path cost 20000, Port priority 128, Port Identifier 128.1.
  Designated root has priority 32769, address 5c71.0dfe.8380
  Designated bridge has priority 32769, address 5c71.0dfe.8380
  Designated port id is 128.1, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 208695, received 1

Port 18 (GigabitEthernet1/0/18) of VLAN0001 is designated forwarding
!
!
<<output truncated>>

```

次に、ポートステータスのサマリーを表示する例を示します。

```

Device#
show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID                is enabled
Portfast Default                   is disabled
PortFast BPDU Guard Default       is disabled
Portfast BPDU Filter Default      is disabled
Loopguard Default                  is disabled
EtherChannel misconfig guard      is enabled
UplinkFast                         is disabled
BackboneFast                       is enabled but inactive in rapid-pvst mode
Configured Pathcost method used is long

Name                               Blocking Listening Learning Forwarding STP Active
-----
VLAN0001                           1           0           0           26          27
-----
1 vlan                             1           0           0           26          27
-----

```

次の例では、スパニングツリーステータスセクションのすべての行を表示する方法を示します。

```

Device#
show spanning-tree summary total Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID                is enabled
Portfast Default                   is disabled
PortFast BPDU Guard Default       is disabled
Portfast BPDU Filter Default      is disabled
Loopguard Default                  is disabled

```

show spanning-tree

```

EtherChannel misconfig guard          is enabled
UplinkFast                            is disabled
BackboneFast                          is enabled but inactive in rapid-pvst mode
Configured Pathcost method used is long

```

```

Name                               Blocking Listening Learning Forwarding STP Active
-----
1 vlan                               1           0           0           26           27

```

次に、特定の VLAN のスパニングツリーに関する情報を表示する例を示します。

```

Device#
show spanning-tree vlan 200
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
            Address     5c71.0dfe.8380
            This bridge is the root
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     5c71.0dfe.8380
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

```

```

Interface          Role Sts Cost      Prio.Nbr Type
-----
Gi1/0/1            Desg FWD 20000    128.1   P2p
Gi1/0/18           Desg FWD 20000    128.18  P2p
Gi1/0/21           Desg FWD 20000    128.21  P2p
Te1/0/25           Desg FWD 20000    128.25  P2p
Te1/0/37           Desg FWD 2000    128.37  P2p
Te1/0/38           Desg FWD 2000    128.38  P2p
Te1/0/45           Desg FWD 20000    128.45  P2p
Te1/0/48           Desg FWD 20000    128.48  P2p
!
!
<<output truncated>>

```

次の表に、この例で表示されるフィールドについて説明します。

Table 103: show spanning-tree vlan コマンドの出力フィールド

フィールド	定義
Role	現在の 802.1w ロール。有効値は、Boun (boundary)、Desg (designated)、Root、Altn (alternate)、および Back (backup) です。
Sts	スパニングツリーステート: 有効値は BKN* (broken) ¹ 、BLK (blocking)、DWN (down)、LTN (listening)、LBK (listening)、LRN (learning)、および FWD (learning) です。
Cost	ポート コスト
Prio.Nbr	ポート プライオリティとポート番号で構成されるポート ID

フィールド	定義
Status	<p>ステータス情報。有効値は次のとおりです。</p> <ul style="list-style-type: none"> • P2p/Shr: スパニングツリーは、このインターフェイスを（共有された）ポイントツーポイントインターフェイスと見なします。 • Edge: PortFast が設定され（default コマンドをグローバルに使用して、または直接インターフェイス上でのいずれか）、BPDU は受信されていません。 • *ROOT_Inc、*LOOP_Inc、*PVID_Inc、および*TYPE_Inc: ポートは不整合のため故障状態（BKN*）です。ポートは（それぞれ）ルート不整合、ループガード不整合、PVID（ポート VLAN ID）不整合、またはタイプ不整合です。 • Bound(type): MST モードで、境界ポートを識別し、ネイバーのタイプ（STP、RSTP、または PVST）を指定します。 • Peer(STP): PVRST rapid-pvst モードで、前のバージョンの 802.1D ブリッジに接続されているポートを識別します。

¹ * については、ステータスフィールドの定義を参照

show spanning-tree mst

マルチスパンニングツリー（MST）プロトコルを表示するには、特権 EXEC モードで **show spanning-tree mst** コマンドを使用します。

show spanning-tree mst [**configuration** [**digest**] | *instance-id-number*] [**interface** *interface*] [**detail**] [**service** *instance*]

Syntax Description

<i>instance-id-number</i>	（任意）インスタンス ID 番号。有効な範囲は 0 ～ 4094 です。
detail	（任意）MST プロトコルに関する詳細情報を表示します。
<i>interface</i>	（任意）インターフェイスに関する情報を表示します。有効な数値については、「“使用上のガイドライン”」セクションを参照してください。
configuration	（任意）リージョン コンフィギュレーション情報を表示します。
digest	（任意）現在の MST 設定 ID（MSTCI）に含まれる Message Digest 5（MD5）アルゴリズムに関する情報を表示します。
interface	（任意）インターフェイスタイプに関する情報を表示します。

Command Modes

特権 EXEC（#）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

interface 引数の有効値は、指定したインターフェイスタイプおよび使用されているシャーシおよびモジュールによって決まります。たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 2 ～ 13、ポート番号の有効値は 1 ～ 48 になります。

port-channel number の有効値は、1 ～ 282 の範囲の最大 64 個の値です。257 ～ 282 の **port-channel number** 値は、コンテンツ スイッチング モジュール（CSM）およびファイアウォール サービス モジュール（FWSM）でのみサポートされています。

vlan の有効値は 1 ～ 4094 です。

show spanning-tree mst configuration コマンドの出力表示に、警告メッセージが表示されることがあります。このメッセージは、セカンダリ VLAN を、関連付けられているプライマリ VLAN と同じインスタンスにマッピングしなかった場合に表示されます。表示には、関連付けられているプライマリ VLAN と同じインスタンスにマッピングされていないセカンダリ VLAN のリストが含まれます。警告メッセージは次のとおりです。

These secondary vlans are not mapped to the same instance as their primary:
-> 3

出力がポート単位で同時に標準ブリッジと先行標準ブリッジの両方に適用される場合、**show spanning-tree mst configuration digest** コマンドの出力表示に、2つの異なるダイジェストが表示されます。

先行標準の PortFast ブリッジプロトコルデータユニット (BPDU) だけを送信するようにポートを設定する場合、先行標準フラグが **show spanning-tree** コマンドに表示されます。先行標準フラグの種類は次のとおりです。

- Pre-STD または pre-standard (長形式) : ポートが先行標準 BPDU を送信するように設定されている場合、およびこのインターフェイス上で先行標準ネイバーブリッジが検出された場合に、このフラグが表示されます。
- Pre-STD-Cf または pre-standard (config) (長形式) : 先行標準 BPDU を送信するようにポートを設定し、そのポートで先行標準 BPDU が受信されない場合、自動検出メカニズムが失敗した場合、または先行標準ネイバーが存在しない場合に設定が間違っている場合、このフラグが表示されます。
- Pre-STD-Rx または pre-standard (rcvd) (長形式) : 先行標準 BPDU がポートで受信され、先行標準 BPDU を送信するようにポートを設定していない場合に、このフラグが表示されます。ポートは先行標準 BPDU を送信しますが、先行標準ネイバーとのやりとりを自動検出メカニズムだけに依存しないようにポートの設定を変更することを推奨します。

設定が先行標準に適合していない場合 (たとえば、単一の MST インスタンス ID が 16 以上の場合)、先行標準ダイジェストは計算されず、次の出力が表示されます。

```
Device# show spanning-tree mst configuration digest

Name      [region1]
Revision  2          Instances configured 3
Digest    0x3C60DBF24B03EBF09C5922F456D18A03
Pre-std Digest  N/A, configuration not pre-standard compatible
```

MST BPDU には、リージョン名、リージョンリビジョン、および MST コンフィギュレーションの VLAN とインスタンス間マッピングの MD5 ダイジェストで構成される MSTCI が含まれます。

出力の説明については、**show spanning-tree mst** コマンドフィールド説明の表を参照してください。

Examples

次に、リージョン設定に関する情報を表示する例を示します。

```
Device# show spanning-tree mst configuration

Name      [train]
Revision  2702
Instance  Vlans mapped
-----
0         1-9,11-19,21-29,31-39,41-4094
1         10,20,30,40
-----
```

次に、追加の MST プロトコル値を表示する例を示します。

```

Device# show spanning-tree mst 3 detail

##### MST03 vlans mapped: 3,3000-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03
GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0
FastEthernet4/1 of MST03 is designated forwarding
Port info port id 128.193 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 254, received 1
FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252

```

次に、現在の MSTCI に含まれている MD5 ダイジェストを表示する例を示します。

```

Device# show spanning-tree mst configuration digest

Name      [mst-config]
Revision  10      Instances configured 25
Digest    0x40D5ECA178C657835C83BBCE16723192
Pre-std Digest 0x27BF112A75B72781ED928D9EC5BB4251

```

Related Commands

コマンド	説明
spanning-tree mst	任意の MST インスタンスのパス コストおよびポートプライオリティ パラメータを設定します。
spanning-tree mst forward-time	Cisco 7600 シリーズルータ上のすべてのインスタンスに対して転送遅延タイマーを設定します。
spanning-tree mst hello-time	Cisco 7600 シリーズルータ上のすべてのインスタンスに対してハロータイム遅延タイマーを設定します。
spanning-tree mst max-hops	BPDU が廃棄される前に領域内で可能なホップカウントを指定します。

show uddl

すべてのポートまたは指定されたポートの単方向リンク検出 (UDLD) の管理ステータスおよび動作ステータスを表示するには、ユーザ EXEC モードで **show uddl** コマンドを使用します。

```
show uddl [Auto-Template | Capwap | GigabitEthernet | GroupVI | InternalInterface |
Loopback | Null | Port-channel | TenGigabitEthernet | Tunnel | Vlan] interface_number
show uddl neighbors
```

Syntax Description	
Auto-Template	(任意) 自動テンプレートインターフェイスの UDLD 動作ステータスを表示します。範囲は 1 ~ 999 です。
Capwap	(任意) CAPWAP インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ~ 2147483647 です。
GigabitEthernet	(任意) GigabitEthernet インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ~ 9 です。
GroupVI	(任意) グループ仮想インターフェイスの UDLD 動作ステータスを表示します。範囲は 1 ~ 255 です。
InternalInterface	(任意) 内部インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ~ 9 です。
Loopback	(任意) ループバック インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ~ 2147483647 です。
Null	(任意) null インターフェイスの UDLD 動作ステータスを表示します。
Port-channel	(任意) イーサネット チャネル インターフェイスの UDLD 動作ステータスを表示します。 指定できる範囲は 1 ~ 48 です。
TenGigabitEthernet	(任意) 10 ギガビットイーサネットインターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ~ 9 です。
Tunnel	(任意) トンネルインターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ~ 2147483647 です。
Vlan	(任意) VLAN インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 1 ~ 4095 です。

interface-id (任意) インターフェイスの ID およびポート番号です。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。

neighbors (任意) ネイバー情報だけを表示します。

Command Modes ユーザ EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines インターフェイス ID を入力しない場合は、すべてのインターフェイスの管理上および運用上の UDLD ステータスが表示されます。

次の例では、**show udld interface-id** コマンドの出力を示します。ここでは、UDLD はリンクの両端でイネーブルに設定されていて、リンクが双方向であることを UDLD が検出します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

Table 104: show udld のフィールドの説明

フィールド	説明
Interface	UDLD に設定されたローカル デバイスのインターフェイス。

フィールド	説明
Port enable administrative configuration setting	ポートでのUDLDの設定方法。UDLDがイネーブルまたはディセーブルの場合、ポートのイネーブル設定は運用上のイネーブルステートと同じです。それ以外の場合、イネーブル動作設定は、グローバルなイネーブル設定によって決まります。
Port enable operational state	このポートでUDLDが実際に稼働しているかどうかを示す動作ステート。
Current bidirectional state	リンクの双方向ステート。リンクがダウンしているか、またはUDLD非対応デバイスに接続されている場合は、unknownステートが表示されます。リンクがUDLD対応デバイスに通常どおり双方向接続されている場合は、bidirectionalステートが表示されます。その他の値が表示されている場合は、正しく配線されていません。
Current operational state	UDLDステートマシンの現在のフェーズ。通常の双方向リンクの場合、多くは、ステートマシンはアドバタイズフェーズです。
Message interval	ローカルデバイスからアドバタイズメッセージを送信する頻度。単位は秒です。
Time out interval	検出ウィンドウ中に、UDLDがネイバーデバイスからのエコーを待機する期間（秒）。
Entry 1	最初のキャッシュエントリの情報。このエントリには、ネイバーから受信されたエコー情報のコピーが格納されます。
Expiration time	このキャッシュエントリの期限が切れるまでの存続期間（秒）。
Device ID	ネイバー デバイスの ID。
Current neighbor state	ネイバーの現在の状態。ローカルデバイスおよびネイバー装置の両方でUDLDが通常どおり稼働している場合、ネイバーステートおよびローカルステートは双方向です。リンクがダウンしているか、またはネイバーがUDLD対応でない場合、キャッシュエントリは表示されません。

フィールド	説明
デバイス名	装置名またはネイバーのシステム シリアル番号。装置名が設定されていないか、またはデフォルト (Switch) に設定されている場合、システムのシリアル番号が表示されます。
Port ID	UDLD に対してイネーブルに設定されたネイバーのポート ID。
Neighbor echo 1 device	エコーの送信元であるネイバーのネイバーデバイス名。
Neighbor echo 1 port	エコーの送信元であるネイバーのポート番号 ID。
Message interval	ネイバーがアドバタイズメッセージを送信する速度 (秒)。
CDP device name	CDP デバイス名またはシステムシリアル番号。装置名が設定されていないか、またはデフォルト (Switch) に設定されている場合、システムのシリアル番号が表示されます。

次に、**show udld neighbors** コマンドの出力例を示します。

```
Device> enable
Device# show udld neighbors
Port      Device Name      Device ID  Port-ID  OperState
-----
Gi2/0/1   Switch-A         1          Gi2/0/1  Bidirectional
Gi3/0/1   Switch-A         2          Gi3/0/1  Bidirectional
```

spanning-tree backbonefast

BackboneFast をイネーブルにして、スイッチ上のブロックされたポートを即座にリスニングモードに切り替えられるようにするには、グローバルコンフィギュレーションモードで **spanning-tree backbonefast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree backbonefast
no spanning-tree backbonefast

Syntax Description

このコマンドには、引数またはキーワードはありません。

Command Default

BackboneFast はディセーブルです。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

イーサネットスイッチネットワーク モジュールを含む Cisco デバイスすべてで BackboneFast をイネーブルにする必要があります。BackboneFast は、スパニングツリーのトポロジ変更後、ネットワーク バックボーンに高速コンバージェンスを提供します。これにより、スイッチは間接リンク障害を検出し、通常のスパニングツリールールを使用している場合よりも早く、スパニングツリーの再設定を開始できるようになります。

設定を確認するには、**show spanning-tree** 特権 EXEC コマンドを使用します。

Examples

次に、デバイスで BackboneFast をイネーブルにする例を示します。

```
Device(config)# spanning-tree backbonefast
```

Related Commands

コマンド	説明
show spanning-tree	スパニングツリーステートに関する情報を表示します。

spanning-tree bpdudfilter

インターフェイス上でブリッジプロトコルデータユニット（BPDU）フィルタリングをイネーブるには、インターフェイス コンフィギュレーション モードまたはテンプレート コンフィギュレーション モードで **spanning-tree bpdudfilter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree bpdudfilter { enable | disable }
no spanning-tree bpdudfilter

Syntax Description	enable	インターフェイスでの BPDU フィルタリングをイネーブるにします。
	disable	インターフェイスでの BPDU フィルタリングをディセーブるにします。
Command Default	spanning-tree portfast edge bpdudfilter default コマンドの入力時点ですでに設定されている設定。	
Command Modes	インターフェイス コンフィギュレーション（config-if） テンプレート コンフィギュレーション（config-template）	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Caution

spanning-tree bpdudfilter enable コマンドを入力するときは注意してください。インターフェイス上でBPDUフィルタリングをイネーブるにすることは、このインターフェイスのスパニングツリーをディセーブるにすることと類似しています。このコマンドを正しく使用しない場合、ブリッジングループが発生する可能性があります。

spanning-tree bpdudfilter enable コマンドを入力してBPDUフィルタリングをイネーブるにすると、PortFast 設定が無効になります。

すべてのサービス プロバイダー エッジ スイッチにレイヤ 2 プロトコル トネリングを設定する場合は、**spanning-tree bpdudfilter enable** コマンドを入力して、802.1Q トネルポート上でスパニングツリー BPDU フィルタリングをイネーブるにする必要があります。

BPDU フィルタリングにより、ポートはBPDUを送受信できなくなります。この設定は、インターフェイスがトランッキングであるかどうかに関係なく、そのインターフェイス全体に適用できます。このコマンドには次の3つの状態があります。

- **spanning-tree bpdudfilter enable:** インターフェイス上の BPDU フィルタリングを無条件にイネーブるにします。

- **spanning-tree bpdudfilter disable:** インターフェイス上のBPDUフィルタリングを無条件にディセーブルにします。
- **no spanning-tree bpdudfilter:** 動作中の PortFast インターフェイスに **spanning-tree portfast bpdudfilter default** コマンドが設定されている場合、そのインターフェイスでBPDUフィルタリングをイネーブルにします。

PortFast 用に設定済みのすべてのポートでBPDUフィルタリングをイネーブルにするには、**spanning-tree portfast bpdudfilter default** コマンドを使用します。

Examples

次に、現在のインターフェイス上でBPDUフィルタリングをイネーブルにする例を示します。

```
Device(config-if)# spanning-tree bpdudfilter enable
Device(config-if)#
```

次に、インターフェイス テンプレートを使用してインターフェイスでBPDUフィルタリングをイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# template user-templatel
Device(config-template)# spanning-tree bpdudfilter enable
Device(config-template)# end
```

Related Commands

コマンド	説明
show spanning-tree	スパニングツリーステートに関する情報を表示します。
spanning-tree portfast edge bpdudfilter default	すべての PortFast ポートで、BPDUフィルタリングをデフォルトでイネーブルにします。

spanning-tree bpduguard

インターフェイス上でブリッジプロトコルデータユニット（BPDU）ガードをイネーブルにするには、インターフェイス コンフィギュレーション モードおよびテンプレート コンフィギュレーションモードで **spanning-tree bpduguard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree bpduguard { enable | disable }
no spanning-tree bpduguard
```

Syntax Description	enable	disable
	インターフェイス上での BPDU ガードをイネーブルにします。	インターフェイス上での BPDU ガードをディセーブルにします。

Command Modes インターフェイス コンフィギュレーション（config-if）
テンプレート コンフィギュレーション（config-template）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines BPDU ガードを使用すると、ポートは BPDU を受信できなくなります。通常、この機能は、アクセスポートがスパンニングツリーに参加しないようにネットワーク管理者によって設定されるサービスプロバイダーの環境で使用されます。ポートが引き続き BPDU を受信する場合は、保護対策としてポートが **error-disabled** ステートに置かれます。このコマンドには次の 3 つの状態があります。

- **spanning-tree bpduguard enable:** インターフェイスで BPDU ガードを無条件でイネーブルにします。
- **spanning-tree bpduguard disable:** インターフェイスで BPDU ガードを無条件でディセーブルにします。
- **no spanning-tree bpduguard:** インターフェイスが PortFast 動作ステートにある場合、および **spanning-tree portfast bpduguard default** コマンドが設定されている場合、インターフェイス上で BPDU ガードがイネーブルになります。

Examples

次の例では、インターフェイス上で BPDU ガードをイネーブルにする方法を示します。

```
Device(config-if)# spanning-tree bpduguard enable
Device(config-if)#
```

次に、インターフェイス テンプレートを使用してインターフェイスで BPDU ガードをイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# template user-templatl
Device(config-template)# spanning-tree bpduguard enable
Device(config-template)# end
```

Related Commands

コマンド	説明
show spanning-tree	スパニングツリーステートに関する情報を表示します。
spanning-tree portfast edge bpduguard default	すべての PortFast ポートで、BPDU ガードをデフォルトでイネーブルにします。

spanning-tree bridge assurance

デバイスのすべてのネットワークポートで Bridge Assurance をイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree bridge assurance** コマンドを使用します。Bridge Assurance をディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree bridge assurance
no spanning-tree bridge assurance

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default Bridge Assurance はイネーブルになっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines Bridge Assurance は、単方向リンク障害または他のソフトウェア障害、およびスパニングツリーアルゴリズムの停止後もデータトラフィックを転送し続けているデバイスから、ネットワークを保護します。

Bridge Assurance は、ポイントツーポイントリンクであるスパニング ツリー ネットワーク ポートでのみイネーブルになります。Bridge Assurance はリンクの両端で常にイネーブルにする必要があります。リンクの一端のデバイスで Bridge Assurance がイネーブルであっても、他端のデバイスが Bridge Assurance をサポートしていない、または Bridge Assurance がイネーブルではない場合、接続ポートはブロックされます。

Bridge Assurance をディセーブルにすると、すべての設定済みネットワークポートが標準のスパニングツリーポートとして動作します。

Examples

次に、スイッチのすべてのネットワークポートで Bridge Assurance をイネーブルにする例を示します。

```
Device(config)#
spanning-tree bridge assurance
Device(config)#
```

次に、スイッチのすべてのネットワークポートで Bridge Assurance をディセーブルにする例を示します。

```
Device(config)#
no spanning-tree bridge assurance
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree	スパニングツリーステートに関する情報を表示します。

spanning-tree cost

スパニングツリープロトコル（STP）計算に使用するインターフェイスのパスコストを設定するには、インターフェイス コンフィギュレーション モードで **spanning-tree cost** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree cost *cost*
no spanning-tree cost

Syntax Description

<i>cost</i>	パス コスト。有効な範囲は1～200000000 です。
-------------	------------------------------

Command Modes

インターフェイス コンフィギュレーション（config-if）
 テンプレート コンフィギュレーション（config-template）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

引数 *cost* の値を指定する場合、値が大きいほどコストは高くなります。指定されたプロトコルタイプに関係なく、この値が適用されます。

ループが発生した場合、スパニングツリーはパスコストを使用して、フォワーディングステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。

Examples

次に、インターフェイスにアクセスし、このインターフェイスに関連するスパニングツリー VLAN にパス コスト値 250 を設定する例を示します。

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree cost 250
```

次に、インターフェイス テンプレートを使用して、インターフェイスに関連するスパニングツリー VLAN にパスコスト値 250 を設定する例を示します。

```
Device# configure terminal
Device(config)# template user-templatel
Device(config-template)# spanning-tree cost 250
Device(config-template)# end
```

Related Commands

コマンド	説明
show spanning-tree	指定されたスパニングツリーインスタンスのスパニングツリー情報を表示します。

コマンド	説明
spanning-tree port-priority	2つのブリッジがルートブリッジとなるために競合している場合に、インターフェイスにプライオリティを設定します。
spanning-tree portfast (グローバル)	リンクがアップした時点で、インターフェイスがタイマーの経過を待たずにただちにフォワーディングステートに移行した場合に、PortFast モードをイネーブルにします。
spanning-tree portfast (インターフェイス)	リンクがアップした時点で、インターフェイスがタイマーの経過を待たずにただちにフォワーディングステートに移行した場合に、PortFast モードをイネーブルにします。
spanning-tree uplinkfast	UplinkFast 機能をイネーブルにします。
spanning-tree vlan	STP を VLAN 単位で設定します。

spanning-tree etherchannel guard misconfig

チャンネルの設定ミスによるループが検出された場合に、エラーメッセージを表示するには、グローバル コンフィギュレーション モードで **spanning-tree etherchannel guard misconfig** コマンドを使用します。エラーメッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree etherchannel guard misconfig
no spanning-tree etherchannel guard misconfig

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default エラー メッセージが表示されます。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines EtherChannel はポート集約プロトコル (PAgP)、または Link Aggregation Control Protocol (LACP) を使用し、インターフェイスの EtherChannel モードが **channel-group group-number mode on** コマンドを使用してイネーブル化されている場合は機能しません。

spanning-tree etherchannel guard misconfig コマンドは、設定不備と誤接続の 2 種類のエラーを検出します。設定不備エラーは、ポートチャンネルと個々のポート間のエラーです。誤接続エラーは、複数のポートをチャネリングしているデバイスと、エラーを検出するのに十分なスパニングツリープロトコル (STP) のブリッジプロトコルデータ ユニット (BPDU) を使用していないデバイスとの間のエラーです。このエラーでは、スイッチが非ルートデバイスである場合にのみ、デバイスは EtherChannel をエラーディセーブルにします。

EtherChannel ガードの設定ミスが検出されると、次のエラー メッセージが表示されます。

```
msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel misconfiguration of %s %s")
```

不良構成に関与しているローカルポートを特定するには、**show interfaces status err-disabled** コマンドを入力します。リモート装置の EtherChannel 設定を調べるには、リモート装置上で **show etherchannel summary** コマンドを入力します。

設定を修正したら、対応するポートチャンネル インターフェイス上で **shutdown** コマンドと **no shutdown** コマンドを入力します。

Examples

次に、EtherChannel ガードの設定ミス機能をイネーブルにする例を示します。

```
Device(config)# spanning-tree etherchannel guard misconfig
Device(config)#
```

Related Commands

コマンド	説明
show etherchannel summary	チャンネルの EtherChannel 情報を表示します。
show interfaces status err-disabled	インターフェイス ステータスを表示したり、LAN ポートで errdisable ステートにあるインターフェイスだけのリストを表示したりします。
shutdown	インターフェイスをディセーブルにします。

spanning-tree extend system-id

1024 個の MAC（メディア アクセス コントロール）アドレスをサポートするシャーシ上で拡張システム ID 機能をイネーブルにするには、グローバルコンフィギュレーションモードで **spanning-tree extend system-id** コマンドを使用します。拡張システム ID をディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree extend system-id
no spanning-tree extend system-id

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

1024 個の MAC アドレスをサポートしないシステム上でイネーブルです。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

拡張システム ID をイネーブルまたはディセーブルにすると、すべてのアクティブなスパニングツリープロトコル（STP）インスタンスのブリッジ ID が更新されるため、これによってスパニングツリー トポロジーが変更される場合があります。

Examples

次に、拡張システム ID をイネーブルにする例を示します。

```
Device(config)# spanning-tree extend system-id
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree	スパニングツリーステートに関する情報を表示します。

spanning-tree guard

ガードモードをイネーブルまたはディセーブルにするには、インターフェイス コンフィギュレーション モードまたはテンプレート コンフィギュレーション モードで **spanning-tree guard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree guard { loop | root | none }
no spanning-tree guard
```

Syntax Description	loop	root	none
	インターフェイスでループ ガードモードをイネーブルにします。	インターフェイスでルートガードモードをイネーブルにします。	ガードモードを None に設定します。

Command Default ガードモードはディセーブルです。

Command Modes インターフェイス コンフィギュレーション (config-if)
 テンプレート コンフィギュレーション (config-template)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples 次の例では、ルート ガードをイネーブルにする方法を示します。

```
Device(config-if)# spanning-tree guard root
Device(config-if)#
```

次の例は、インターフェイス テンプレートを使用してインターフェイスでルートガードをイネーブルにする方法を示しています。

```
Device# configure terminal
Device(config)# template user-templaten1
Device(config-template)# spanning-tree guard root
Device(config-template)# end
```

Related Commands	コマンド	説明
	show spanning-tree	スパニングツリー ステートに関する情報を表示します。
	spanning-tree loopguard default	所定のブリッジのすべてのポート上でデフォルトとしてループガードをイネーブルにします。

spanning-tree link-type

ポートにリンクタイプを設定するには、インターフェイスコンフィギュレーションモードおよびテンプレート コンフィギュレーション モードで **spanning-tree link-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree link-type { **point-to-point** | **shared** }
no spanning-tree link-type

Syntax Description

point-to-point	インターフェイスがポイントツーポイントリンクになるように指定します。
shared	インターフェイスが共有メディアになるように指定します。

Command Default

リンク タイプは、明示的に設定しなければ、デュプレックス設定から自動的に生成されます。

Command Modes

インターフェイス コンフィギュレーション (config-if)
 テンプレート コンフィギュレーション (config-template)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Rapid Spanning Tree Protocol Plus (RSTP+) 高速トランジションが機能するのは、2つのブリッジ間のポイントツーポイントリンク上だけです。

デフォルトでは、スイッチはデュプレックスモードからポートのリンクタイプを判断します。つまり、全二重ポートはポイントツーポイントリンクと見なされ、半二重設定は共有リンク上にあると見なされます。

ポートを共有リンクとして指定した場合は、デュプレックス設定に関係なく、RSTP+ 高速トランジションは禁止されます。

ポート（ローカルポート）をポイントツーポイントリンクでリモートポートと接続し、ローカルポートが指定ポートになると、デバイスはリモートポートとネゴシエーションし、ローカルポートをフォワーディングステートにすばやく変更します。

Examples

次に、ポートを共有リンクとして設定する例を示します。

```
Device(config-if)# spanning-tree link-type shared
Device(config-if)#
```

次に、インターフェイス テンプレートを使用してポートを共有リンクとして設定する例を示します。

```
Device# configure terminal
```

```
Device(config)# template user-templatl  
Device(config-template)# spanning-tree link-type shared  
Device(config-template)# end
```

Related Commands

コマンド	説明
show spanning-tree interface	スパニングツリーステートに関する情報を表示します。

spanning-tree loopguard default

指定されたブリッジのすべてのポート上でループガードをデフォルトでイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree loopguard default** コマンドを使用します。ループガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree loopguard default
no spanning-tree loopguard default

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default ループ ガードはディセーブルです。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ループガードを使用すると、ブリッジネットワークのセキュリティを高めることができます。また、単方向リンクの原因となる障害によって代替ポートまたはルートポートが指定ポートとして使用されることがなくなります。

ループガードが動作するのは、スパニングツリーがポイントツーポイントと見なすポート上だけです。

ループガード ポートを個別に設定すると、このコマンドが上書きされます。

Examples

次に、ループ ガードをイネーブルにする例を示します。

```
Device(config)# spanning-tree loopguard default
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。
spanning-tree guard	ガードモードをイネーブルまたはディセーブルにします。

spanning-tree mode

Per-VLAN Spanning Tree+ (PVST+)、Rapid-PVST+、およびマルチスパンニングツリー (MST) モードの間で切り替えるには、グローバルコンフィギュレーションモードで **spanning-tree mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mode [pvst | mst | rapid-pvst]
no spanning-tree mode

Syntax Description	pvst	(任意) PVST+ モード
	mst	(任意) MST モード
	rapid-pvst	(任意) 高速 PVST+ モード
Command Default	pvst	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Note **spanning-tree mode** コマンドを使用して PVST+、Rapid-PVST+、および MST モードを切り替える場合は、慎重に行ってください。このコマンドを入力すると、以前のモードのスパンニングツリーインスタンスはすべて停止し、新しいモードで再開されます。このコマンドを使用すると、ユーザトラフィックが中断されることがあります。

Examples

次に、MST モードに切り替える例を示します。

```
Device(config)# spanning-tree mode mst
Device(config)#
```

次に、デフォルトモード (PVST+) に戻す例を示します。

```
Device(config)# no spanning-tree mode
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst

プライオリティパラメータを設定するか、デバイスをマルチスパンニングツリー（MST）インスタンスのルートとして設定するには、インターフェイス コンフィギュレーション モードで **spanning-tree mst** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree mst instance-id { priority priority | root { primary | secondary } }
no spanning-tree mst instance-id { { priority priority | root { primary | secondary } } }
```

Syntax Description

priority <i>priority</i>	1つのインスタンスのポートプライオリティ。指定できる範囲は0～61440で、4096ずつ増加します。
root	デバイスをルートとして設定します。

Command Modes

インターフェイス コンフィギュレーション（config-if）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、プライオリティを設定する例を示します。

```
Device(config-if)#
spanning-tree mst 0 priority 1
Device(config-if)#
```

次に、デバイスをプライオリティルートとして設定する例を示します。

```
Device(config-if)#
spanning-tree mst 0 root primary
Device(config-if)#
```

Related Commands

コマンド	説明
show spanning-tree mst	MSTプロトコルに関する情報を表示します。

spanning-tree mst configuration

MST コンフィギュレーション サブモードを開始するには、グローバル コンフィギュレーション モードで **spanning-tree mst configuration** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst configuration
no spanning-tree mst configuration

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

デフォルトでは、マルチスパンニングツリー (MST) の設定値がすべてのパラメータのデフォルト値になります。

- VLAN はどの MST インスタンスにもマッピングされません (すべての VLAN は Common and Internal Spanning Tree [CIST] インスタンスにマッピングされます)。
- 領域名は空の文字列になります。
- リビジョン番号は 0 です。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

MST コンフィギュレーションは、次の 3 つの主要パラメータから構成されます。

- インスタンス VLAN マッピング (**instance** コマンドを参照)。
- リージョン名: **name** コマンド (MST コンフィギュレーション サブモード) を参照。
- コンフィギュレーション リビジョン番号 (**revision** コマンドを参照)。

MST コンフィギュレーション サブモードは、**abort** コマンドと **exit** コマンドで終了できます。これら 2 つのコマンドの違いは、変更内容を保存するかどうかです。

exit コマンドは、MST コンフィギュレーション サブモードを終了する前に、すべての変更内容をコミットします。セカンダリ VLAN が、対応付けられたプライマリ VLAN と同じインスタンスにマッピングされていない場合に、MST コンフィギュレーション サブモードを終了すると、警告メッセージが表示され、対応付けられたプライマリ VLAN と同じインスタンスにマッピングされていないセカンダリ VLAN が一覧表示されます。警告メッセージは次のとおりです。

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

abort コマンドは、変更を実行しないで、MST コンフィギュレーション サブモードを終了します。

MST コンフィギュレーション サブモード パラメータを変更すると、接続損失が発生する可能性があります。サービスの中断を減らすには、MST コンフィギュレーション サブモードを開始する場合、現在の MST コンフィギュレーションのコピーを変更します。コンフィギュレーションの編集が終了したら、**exit** キーワードを使用してすべての変更内容を一度に適用するか、または **abort** キーワードを使用して変更をコンフィギュレーションにコミットせずにサブモードを終了します。

2名のユーザがまったく同時に新しいコンフィギュレーションを実行することは通常ありませんが、その場合は次の警告メッセージが表示されます。

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

次に、MST コンフィギュレーション サブモードを開始する例を示します。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)#
```

次の例では、MST コンフィギュレーションをデフォルト設定にリセットする方法を示します。

```
Device(config)# no spanning-tree mst configuration
Device(config)#
```

Related Commands

コマンド	説明
instance	VLAN または VLAN セットを MST インスタンスにマッピングします。
name (MST)	MST リージョンの名前を設定します。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst forward-time

転送遅延タイマーをデバイス上のすべてのインスタンスに設定するには、グローバル コンフィギュレーションモードで **spanning-tree mst forward-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst forward-time *seconds*
no spanning-tree mst forward-time

Syntax Description	<i>seconds</i>	デバイス上のすべてのインスタンスに設定される転送遅延タイマーの秒数。有効な範囲は 4 ~ 30 秒です。
Command Default	15 秒	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、転送遅延タイマーを設定する例を示します。

```
Device(config)# spanning-tree mst forward-time 20
Device(config)#
```

Related Commands	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst hello-time

ハロータイム遅延タイマーをデバイス上のすべてのインスタンスに設定するには、グローバルコンフィギュレーションモードで **spanning-tree mst hello-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst hello-time *seconds*
no spanning-tree mst hello-time

Syntax Description	<i>seconds</i> デバイス上のすべてのインスタンスに設定されるハロータイム遅延タイマーの秒数。有効な範囲は 1 ~ 10 秒です。
---------------------------	---

Command Default 2 秒

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines *hello-time* 値を指定しない場合は、ネットワーク直径から値が計算されます。

Examples

次に、ハロータイム遅延タイマーを設定する例を示します。

```
Device(config)# spanning-tree mst hello-time 3
Device(config)#
```

Related Commands	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst max-age

最大経過時間タイマーをデバイス上のすべてのインスタンスに設定するには、グローバル コンフィギュレーションモードで **spanning-tree mst max-age** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-age *seconds*
no spanning-tree mst max-age

Syntax Description	<i>seconds</i>	デバイス上のすべてのインスタンスに設定される最大経過時間タイマーの秒数。有効な範囲は 6 ~ 40 秒です。
Command Default	20 秒	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、最大経過時間タイマーを設定する例を示します。

```
Device(config)# spanning-tree mst max-age 40
Device(config)#
```

Related Commands	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst max-hops

ブリッジプロトコルデータユニット（BPDU）が廃棄されるまでの領域内の最大ホップ数を指定するには、グローバル コンフィギュレーション モードで **spanning-tree mst max-hops** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-hops *hopnumber*
no spanning-tree mst max-hops

Syntax Description	<i>hopnumber</i>	BPDU が廃棄されるまでに領域内で可能なホップ数。範囲は 1 ～ 255 ホップです。
Command Default	20 hops	
Command Modes	グローバル コンフィギュレーション（config）	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、許容されるホップ数を設定する例を示します。

```
Device(config)# spanning-tree mst max-hops 25
Device(config)#
```

Related Commands	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst pre-standard

先行標準のブリッジプロトコルデータユニット（BPDU）だけを送信するようにポートを設定するには、インターフェイス コンフィギュレーションモードで **spanning-tree mst pre-standard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst pre-standard
no spanning-tree mst pre-standard

Syntax Description	このコマンドには引数またはキーワードはありません。	
Command Default	デフォルトでは、先行標準ネイバーを自動的に検出します。	
Command Modes	インターフェイス コンフィギュレーション（config-if）	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	<p>デフォルト設定であっても、ポートは先行標準および標準 BPDU の両方を受信できます。</p> <p>先行標準 BPDU は、IEEE 標準が完成する前に作成された Cisco IOS マルチ スパニングツリー（MST）実装に基づいています。標準 BPDU は、最終 IEEE 標準に基づいています。</p> <p>先行標準の BPDU だけを送信するようにポートを設定する場合、先行標準フラグが show spanning-tree コマンドに表示されます。先行標準フラグの種類は次のとおりです。</p> <ul style="list-style-type: none"> • Pre-STD または pre-standard（長形式）：ポートが先行標準 BPDU を送信するように設定されている場合、およびこのインターフェイス上で先行標準ネイバーブリッジが検出された場合に、このフラグが表示されます。 • Pre-STD-Cf または pre-standard (config)（長形式）：先行標準 BPDU を送信するようにポートを設定し、そのポートで先行標準 BPDU が受信されない場合、自動検出メカニズムが失敗した場合、または先行標準ネイバーが存在しない場合に設定が間違っている場合、このフラグが表示されます。 • Pre-STD-Rx または pre-standard (rcvd)（長形式）：先行標準 BPDU がポートで受信され、先行標準 BPDU を送信するようにポートを設定していない場合に、このフラグが表示されます。ポートは先行標準 BPDU を送信しますが、先行標準ネイバーとのやりとりを自動検出メカニズムだけに依存しないようにポートの設定を変更することを推奨します。
-------------------------	---

MST の設定が先行標準に適合しない場合（インスタンス ID が 15 より大きい場合）、ポート上の STP の設定に関係なく、標準 MST BPDU だけが送信されます。

Examples

次に、先行標準 BPDU だけを送信するようにポートを設定する例を示します。

```
Router(config-if)# spanning-tree mst pre-standard
Router(config-if)#
```

Related Commands

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst priority

インスタンスのブリッジプライオリティを設定するには、グローバル コンフィギュレーション モードで **spanning-tree mst priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst instance priority priority
no spanning-tree mst priority

Syntax Description	instance	インスタンス ID 番号を指定します。有効値は 0 ～ 4094 です。
	priority priority	ブリッジプライオリティを指定します。有効値および詳細については、「使用上のガイドライン」を参照してください。

Command Default *priority* : 32768

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ブリッジプライオリティは、4096ずつ増分して設定できます。優先順位を設定する場合、有効な値は、**0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344**、および **61440** です。

スイッチをルートにする場合は、*priority* を **0** に設定します。

instance は、単一インスタンスまたはインスタンス範囲 (0 ～ 3、5、7 ～ 9 など) として入力できます。

Examples

次に、ブリッジプライオリティを設定する例を示します。

```
Device(config)# spanning-tree mst 0 priority 4096
Device(config)#
```

Related Commands	コマンド	説明
	show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst root

インスタンスのプライマリルートスイッチおよびセカンダリルートスイッチを指定し、タイマー値を設定するには、グローバル コンフィギュレーション モードで **spanning-tree mst root** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree mst instance root { primary | secondary } [ diameter diameter [ hello-time seconds ] ]
no spanning-tree mst instance root
```

Syntax Description	
<i>instance</i>	インスタンス ID 番号。有効な範囲は 0 ~ 4094 です。
primary	スパニングツリー インスタンスのルートを作成するのに十分な高い優先順位（小さな値）を指定します。
secondary	プライマリ ルートに障害が発生した場合に、セカンダリ ルートとなるようにスイッチを指定します。
diameter <i>diameter</i>	（任意）ネットワークの直径に基づく、ルートスイッチのタイマー値を指定します。指定できる範囲は 1 ~ 7 です。
hello-time <i>seconds</i>	（任意）ルートスイッチが設定メッセージを生成する間隔を指定します。

Command Default **spanning-tree mst root** コマンドには、デフォルト設定はありません。

Command Modes グローバル コンフィギュレーション（config）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines *instance* は、単一インスタンスまたはインスタンス範囲（0 ~ 3、5、7 ~ 9 など）として入力できます。

spanning-tree mst root secondary の値は 16384 です。

diameter *diameter* および **hello-time** *seconds* キーワードと引数は、インスタンス 0 だけに使用できます。

seconds 引数を指定しない場合、この引数の値はネットワークの直径から計算されます。

Examples

次に、インスタンスのプライマリルートスイッチとタイマー値を指定する例を示します。

```
Router(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Router(config)# spanning-tree mst 5 root primary
Router(config)#
```

Related Commands

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree mst simulate pvst global

Per-VLAN Spanning Tree (PVST) シミュレーションをグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree mst simulate pvst global** コマンドを入力します。PVST シミュレーションをグローバルにディセーブルにするには、このコマンドの **no** 形式を入力します。

spanning-tree mst simulate pvst global
no spanning-tree mst simulate pvst global

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

PVST シミュレーションは、イネーブルになっています。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドがサポートされるようになりました。

Usage Guidelines

PVST シミュレーションはデフォルトでイネーブルになっているので、デバイス上のすべてのインターフェイスは多重スパニングツリー (MST) と Rapid Per-VLAN Spanning Tree Plus (PVST+) 間で相互運用されます。MST をデフォルトのスパニングツリープロトコル (STP) モードとして実行していないデバイスに誤って接続するのを避けるには、PVST シミュレーションをディセーブルにします。Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートは、ブロック ステートに移行します。このポートは、ブリッジプロトコルデータユニット (BPDU) の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

ポートのグローバルな PVST シミュレーション設定を上書きするには、インターフェイス コマンド モードで **spanning-tree mst simulate pvst** インターフェイスコマンドを入力します。

Examples

次に、Rapid PVST+ を実行している接続先デバイスとの自動的な相互運用を回避する例を示します。

```
Device(config)#
no spanning-tree mst simulate pvst global
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree pathcost method

デフォルトのパスコスト計算方式を設定するには、グローバルコンフィギュレーションモードで **spanning-tree pathcost method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree pathcost method { long | short }
no spanning-tree pathcost method

Syntax Description	long	デフォルトポートパスコスト用の 32 ビット ベース値を指定します。
	short	デフォルトポートパスコスト用の 16 ビット ベース値を指定します。
Command Default	short	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **long** パスコスト計算方式では、パスコスト計算に 32 ビットをすべて利用して、1 ~ 200000000 の値を生成します。

short パスコスト計算方式 (16 ビット) では、1 ~ 65535 の値を生成します。

Examples

次に、デフォルトのパス コスト計算方式を **long** に設定する例を示します。

```
Device(config)
#) spanning-tree pathcost method long
Device(config)
#)
```

次に、デフォルトのパス コスト計算方式を **short** に設定する例を示します。

```
Device(config)
#) spanning-tree pathcost method short
Device(config)
#)
```

Related Commands	コマンド	説明
	show spanning-tree	スパニングツリーステートに関する情報を表示します。

spanning-tree port-priority

2つのブリッジがルートブリッジとなるために競合している場合に、インターフェイスにプライオリティを設定するには、インターフェイスコンフィギュレーションモードおよびテンプレートコンフィギュレーションモードで **spanning-tree port-priority** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree port-priority *port-priority*
no spanning-tree port-priority

Syntax Description

<i>port-priority</i>	ポートプライオリティです。指定できる範囲は0～240で、16ずつ増加します。デフォルト値は128です。
----------------------	---

Command Default

デフォルトのポートの優先順位は128です。

Command Modes

インターフェイスコンフィギュレーション (config-if)

テンプレートコンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

設定した優先順位により、ルートブリッジとして指定した2つのブリッジ間の関係が解消されません。

Examples

次に、スパニングツリーインスタンス20がインターフェイスイーサネット2/0のルートブリッジとして選択される可能性を高める例を示します。

```
Device(config)# interface ethernet 2/0
Device(config-if)# spanning-tree port-priority 20
Device(config-if)#
```

次に、インターフェイステンプレートを使用して、スパニングツリーインスタンス20がインターフェイスのルートブリッジとして選択される可能性を高める例を示します。

```
Device# configure terminal
Device(config)# template user-templ1
Device(config-template)# spanning-tree port-priority 20
Device(config-template)# end
```

Related Commands

コマンド	説明
show spanning-tree	指定されたスパニングツリー インスタンスのスパニングツリー情報を表示します。
spanning-tree cost	STP 計算に使用するインターフェイスのパスコストを設定します。
spanning-tree portfast (グローバル)	リンクがアップした時点で、インターフェイスがタイマーの経過を待たずにただちにフォワーディングステートに移行した場合に、PortFast モードをイネーブルにします。
spanning-tree uplinkfast	UplinkFast 機能をイネーブルにします。
spanning-tree vlan	STP を VLAN 単位で設定します。

spanning-tree portfast edge bpdudfilter default

すべての PortFast ポートで、ブリッジプロトコルデータユニット (BPDU) フィルタリングをデフォルトでイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree portfast edge bpdudfilter default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast edge bpdudfilter default
no spanning-tree portfast edge bpdudfilter default

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

ディセーブル

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

spanning-tree portfast edge bpdudfilter コマンドは、PortFast ポートで BPDU フィルタリングをグローバルにイネーブルにします。BPDU フィルタリングにより、ポートはいずれの BPDU も送受信できなくなります。

portfast edge bpdudfilter default コマンドを無効にするには、インターフェイスごとに BPDU フィルタリングを設定します。



Note

BPDU フィルタリングをイネーブルにする場合は注意してください。ポート単位でイネーブルにする場合とグローバルにイネーブルする場合では、機能が異なります。グローバルにイネーブル化された BPDU フィルタリングは、PortFast 動作ステータスのポートにのみ適用されます。ポートは数個の BPDU をリンクアップ時に送出してから、実際に、発信 BPDU のフィルタリングを開始します。エッジポートに着信した BPDU は、ただちに PortFast 動作ステータスを失い、BPDU フィルタリングがディセーブルになります。BPDU フィルタリングをポート上でローカルにイネーブルにすると、デバイスがそのポート上で BPDU を送受信しなくなります。



Caution

このコマンドを使用するときは注意してください。このコマンドを誤って使用すると、ブリッジンググループに陥る可能性があります。

Examples

次の例では、BPDU フィルタリングをデフォルトでイネーブルにする方法を示します。

```
Device(config)#  
spanning-tree portfast edge bpdudfilter default  
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree bpdudfilter	インターフェイス上でBPDU フィルタリングをイネーブルにします。

spanning-tree portfast edge bpduguard default

すべての PortFast ポートで、ブリッジプロトコルデータユニット (BPDU) ガードをデフォルトでイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree portfast edge bpduguard default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast edge bpduguard default
no spanning-tree portfast edge bpduguard default

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

ディセーブル

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Caution

このコマンドを使用するときは注意してください。このコマンドを使用するのは、エンドステーションに接続されているインターフェイスでだけにしてください。さもなければ、不慮のトポロジグループからデータ パケットループが発生し、デバイスやネットワークの稼働が中断される可能性があります。

BPDU ガードは、BPDU を受信したポートをディセーブルにします。BPDU ガードは、PortFast がイネーブルに設定されており、PortFast 動作ステートになっているポートに対してのみ適用されません。

Examples

次の例では、BPDU ガードをデフォルトでイネーブルにする方法を示します。

```
Device(config)#
spanning-tree portfast edge bpduguard default
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree mst	MST プロトコルに関する情報を表示します。
spanning-tree bpdudfilter	インターフェイス上で BPDU フィルタリングをイネーブルにします。

spanning-tree portfast default

すべてのアクセスポートで、PortFast をデフォルトでイネーブルにするには、グローバルコンフィギュレーション モードで **spanning-tree portfast {edge | network | normal} default** コマンドを使用します。すべてのアクセスポートで、PortFast をデフォルトでディセーブルにするには、このコマンドの **no** 形式を使用します。

```
spanning-tree portfast { edge [ bpdufilter | bpduguard ] | network | normal } default
no spanning-tree portfast { edge [ bpdufilter | bpduguard ] | network | normal } default
```

Syntax Description

bpdufilter	すべての PortFast ポートで、PortFast エッジ BPDU フィルタリングをデフォルトでイネーブルにします。
bpduguard	すべての PortFast ポートで、PortFast エッジ BPDU ガードをデフォルトでイネーブルにします。
edge	すべてのスイッチポート上で PortFast エッジモードをデフォルトでイネーブルにします。
network	すべてのスイッチポート上で PortFast ネットワークモードをデフォルトでイネーブルにします。
normal	すべてのスイッチポート上で PortFast 通常モードをデフォルトでイネーブルにします。

Command Default

すべてのアクセスポート上で PortFast をデフォルトでディセーブルにします。

Command Modes

グローバル コンフィギュレーション (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Note このコマンドを使用するときは注意してください。このコマンドは、端末に接続されているインターフェイスに対してだけ使用してください。そうでない場合、予想外のトポロジループが原因でデータパケットループが発生し、ルータ、スイッチ、およびネットワークの動作が中断する可能性があります。

リンクがアップすると、PortFast モードがイネーブルに設定されたインターフェイスは標準の転送遅延時間の経過を待たずに、ただちにスパンニングツリー フォワーディング ステートに移行します。

インターフェイスごとに個別に PortFast モードをイネーブルにするには、**spanning-tree portfast** (インターフェイス) コマンドを使用します。

Examples

次に、すべてのアクセスポート上でデフォルトでBPDUガードを備えたを PortFast エッジモードをイネーブルにする例を示します。

```
Device(config)#
spanning-tree portfast edge bpduguard default
Device(config)#
```

Related Commands

コマンド	説明
show spanning-tree	スパニングツリー ステートに関する情報を表示します。
spanning-tree portfast (interface)	特定のインターフェイス上で PortFast をイネーブルにします。

spanning-tree transmit hold-count

送信ホールドカウントを指定するには、グローバルコンフィギュレーションモードで **spanning-tree transmit hold-count** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree transmit hold-count *value*
no spanning-tree transmit hold-count

Syntax Description	<i>value</i>	一時停止するまで 1 秒間に送信されるブリッジプロトコルデータ ユニット (BPDU) の数。有効な範囲は 1 ~ 20 です。
---------------------------	--------------	--

Command Default *value* : 6

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、すべてのスパンニングツリー モードでサポートされています。
 送信ホールド カウントは、一時停止するまで 1 秒間に送信される BPDU の数を決定します。



Note このパラメータをより高い値に変更すると、特に高速 Per-VLAN Spanning Tree (PVST) モードで、CPU 利用率に重大な影響を与える可能性があります。このパラメータを低い値に設定すると、一部のシナリオでコンバージェンスが低速になる可能性があります。デフォルト設定から値を変更しないことを推奨します。

value 設定を変更する場合は、**show running-config** コマンドを入力して、変更内容を確認します。
 コマンドを削除する場合は、**show spanning-tree mst** コマンドを使用して、削除内容を確認します。

Examples

次に、送信ホールド カウントを指定する例を示します。

```
Device(config)# spanning-tree transmit hold-count 8
Device(config)#
```

Related Commands

コマンド	説明
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。

spanning-tree uplinkfast

UplinkFast をイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree uplinkfast** コマンドを使用します。UplinkFast をディセーブルにするには、このコマンドの **no** 形式を使用します。

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]
no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description	max-update-rate <i>packets-per-second</i>	(任意) 更新パケット送信時の最高速度 (1秒あたりのパケット数) を指定します。有効な範囲は 0 ~ 32000 です。
---------------------------	---	---

Command Default	デフォルトの設定は次のとおりです。 <ul style="list-style-type: none"> • UplinkFast はディセーブルです。 • <i>packets-per-second</i> は 150 パケット/秒です。
------------------------	--

Command Modes	グローバル コンフィギュレーション (config)
----------------------	----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	spanning-tree uplinkfast max-update-rate コマンドを使用すると、UplinkFast がイネーブルになり (まだイネーブルでない場合)、更新パケットの送信速度が変更されます。デフォルトの速度に戻すには、このコマンドの no 形式を使用します。
-------------------------	---

Examples	次の例では、UplinkFast をイネーブルにして、最大速度を 200 パケット/秒に設定する方法を示します。
-----------------	--

```
Device(config)#
spanning-tree uplinkfast max-update-rate 200
Device(config)#
```

Related Commands	コマンド	説明
	show spanning-tree	スパニングツリーステートに関する情報を表示します。

spanning-tree vlan

仮想 LAN (VLAN) 単位でスパニングツリープロトコル (STP) を設定するには、グローバル コンフィギュレーションモードで **spanning-tree vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree vlan vlan-id [ forward-time seconds | hello-time seconds | max-age seconds | priority
priority | root [ primary | secondary ] ]
no spanning-tree vlan vlan-id [ forward-time | hello-time | max-age | priority | root ]
```

Syntax Description

<i>vlan id</i>	VLAN ID 番号。指定できる範囲は 1 ~ 4094 です。
forward-time <i>seconds</i>	(任意) STP 転送遅延時間を設定します。有効な範囲は 4 ~ 30 秒です。
hello-time <i>seconds</i>	(任意) ルートスイッチが設定メッセージを生成する間隔を秒単位で指定します。有効な範囲は 1 ~ 10 秒です。
max-age <i>seconds</i>	(任意) ブリッジプロトコルデータユニット (BPDU) 内の情報が有効である最大期間 (秒数) を設定します。有効値の範囲は 6 ~ 40 秒です。
priority <i>priority</i>	(任意) STP ブリッジプライオリティを設定します。有効値の範囲は 0 ~ 65535 です。
root primary	(任意) このスイッチを強制的にルートブリッジにします。
root secondary	(任意) プライマリルートに障害が発生した場合に、このスイッチがルートスイッチとして機能するように指定します。

Command Default

デフォルトは、次のとおりです。

- **forward-time**: 15 秒
- **hello-time**: 2 秒
- **max-age**: 20 秒
- **priority**: IEEE STP がイネーブルの場合のデフォルトは 32768、STP がイネーブルの場合のデフォルトは 128。
- **root**: STP ルートなし

no spanning-tree vlan *vlan_id* コマンドを発行すると、次のパラメータがデフォルトにリセットされます。

- **priority**: IEEE STP がイネーブルの場合のデフォルトは 32768、STP がイネーブルの場合のデフォルトは 128。
- **hello-time**: 2 秒
- **forward-time**: 15 秒

- **max-age:** 20 秒

Command Modes

グローバル コンフィギュレーション (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Caution

- **no spanning-tree vlan *vlan-id*** コマンドを使用して、VLAN 上のスパニングツリーをディセーブルにする場合は、VLAN のすべてのスイッチおよびブリッジのスパニングツリーがディセーブルになっていることを確認してください。VLAN 内の一部のスイッチおよびブリッジのスパニングツリーをディセーブルにし、同じ VLAN 内の別のスイッチおよびブリッジのスパニングツリーをイネーブルにしておくことはできません。なぜなら、スパニング ツリーがイネーブルになっているスイッチおよびブリッジは、ネットワークの物理トポロジについて不完全な情報しか持たないからです。
- 物理的なループの存在しないトポロジであっても、スパニングツリーをディセーブルにすることは推奨しません。スパニング ツリーは誤設定やケーブル障害を防ぐ役割を果たします。VLAN に物理ループが存在しないことを確認せずに、VLAN でスパニング ツリーをディセーブルにしないでください。

max-age *seconds* パラメータが設定されているときに、ブリッジが指定インターバル内にルートブリッジからブリッジプロトコルデータユニット (BPDU) を受信しない場合は、ネットワークが変更されていると見なされ、スパニングツリートポロジが再計算されます。

spanning-tree root primary コマンドを入力すると、スイッチのブリッジプライオリティが 8192 に変更されます。 **spanning-tree root primary** コマンドを入力したにもかかわらず、スイッチがルートスイッチにならなかった場合は、このスイッチのブリッジプライオリティが現在のブリッジのブリッジプライオリティよりも 100 だけ小さい値に変更されます。それでもスイッチがルートにならない場合は、エラーが発生します。

spanning-tree root secondary コマンドを入力すると、スイッチのブリッジプライオリティが 16384 に変更されます。ルートスイッチに障害が発生した場合は、このスイッチが次のルートスイッチになります。

spanning-tree root コマンドは、バックボーンスイッチでのみ使用してください。

spanning-tree etherchannel guard misconfig コマンドは、設定不備と誤接続の 2 種類のエラーを検出します。設定不備エラーは、ポートチャネルと個々のポート間のエラーです。誤接続エラーは、複数のポートをチャネリングしているスイッチと、エラーを検出するのに十分なスパニングツリープロトコル (STP) のブリッジプロトコルデータユニット (BPDU) を使用していないスイッチとの間のエラーです。このエラーでは、スイッチが非ルートスイッチである場合にのみ、スイッチは EtherChannel をエラーディセーブルにします。

Examples

次に、VLAN 200 でスパニングツリーをイネーブルにする例を示します。

```
Device(config)# spanning-tree vlan 200
```

次に、スイッチを VLAN 10 のルートスイッチとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Device(config)# spanning-tree vlan 10 root primary diameter 4
```

次に、スイッチを VLAN 10 のセカンダリルートスイッチとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Device(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Commands

コマンド	説明
spanning-tree cost	STP 計算に使用するインターフェイスのパス コストを設定します。
spanning-tree etherchannel guard misconfig	チャンネルの設定不備によるループが検出されると、エラーメッセージを表示します。
spanning-tree port-priority	2つのブリッジがルートブリッジとなるために競合している場合に、インターフェイスにプライオリティを設定します。
spanning-tree uplinkfast	UplinkFast 機能をイネーブルにします。
show spanning-tree	指定されたスパニングツリー インスタンスのスパニングツリー情報を表示します。

switchport

レイヤ 3 モードになっているインターフェイスをレイヤ 2 設定用のレイヤ 2 モードに配置するには、インターフェイスコンフィギュレーションモードで **switchport** コマンドを使用します。インターフェイスをレイヤ 3 モードに配置するには、このコマンドの **no** 形式を使用します。

switchport
no switchport

Command Default

デフォルトでは、すべてのインターフェイスがレイヤ 2 モードです。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

インターフェイスをルーテッドインターフェイスの状態に設定して、レイヤ 2 の設定をすべて削除するには、**no switchport** コマンド（パラメータの指定なし）を使用します。このコマンドは、ルーテッドポートに IP アドレスを割り当てる前に使用する必要があります。

no switchport コマンドを入力するとポートがシャットダウンされて、その後再び有効になります。その際に、ポートの接続先のデバイスでメッセージが生成されることがあります。

レイヤ 2 モードからレイヤ 3 モード（またはその逆）にインターフェイスを変更すると、影響を受けたインターフェイスに関連する以前の設定情報が失われる可能性があり、インターフェイスがデフォルト設定に戻ります。



Note インターフェイスがレイヤ 3 インターフェイスとして設定されている場合、最初に **switchport** コマンドを入力して、そのインターフェイスをレイヤ 2 ポートとして設定する必要があります。その後、**switchport access vlan** コマンドおよび **switchport mode** コマンドを入力します。

switchport コマンドは、シスコルーテッドポートをサポートしないプラットフォームでは使用できません。このようなプラットフォーム上のすべての物理ポートは、レイヤ 2 のスイッチドインターフェイスとして想定されます。

インターフェイスのポートステータスを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

Examples

次の例では、インターフェイスをレイヤ 2 ポートとして運用することを中止し、シスコのルーテッドポートにする方法を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# no switchport
```

次の例では、ポートのインターフェイスをシスコのルーテッドポートとして運用することを中止し、レイヤ 2 のスイッチドインターフェイスに変更する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport
```

switchport access vlan

ポートをスタティックアクセスポートとして設定するには、インターフェイスコンフィギュレーションモードで **switchport access vlan** コマンドを使用します。デバイスのアクセスモードをデフォルトの VLAN モードにリセットするには、このコマンドの **no** 形式を使用します。

```
switchport access vlan {vlan-id}
no switchport access vlan
```

Syntax Description

vlan-id アクセスモード VLAN の VLAN ID。範囲は 1~4094。

Command Default

デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

switchport access vlan コマンドを有効にするには、事前にポートをアクセスモードにする必要があります。

スイッチポートのモードが **access vlan** *vlan-id* に設定されている場合、ポートは指定された VLAN のメンバとして動作します。アクセスポートを割り当てることができるのは、1つの VLAN だけです。

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます。インターフェイステンプレートの場合は、テンプレートを使用してコマンドを適用する前に、VLAN を明示的に作成してください。

no switchport access コマンドを使用すると、アクセスモード VLAN がデバイスに適したデフォルト VLAN にリセットされます。

Examples

次の例では、アクセスモードで動作するスイッチドポートインターフェイスが、デフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport access vlan 2
```

switchport mode

ポートの VLAN メンバーシップモードを設定するには、インターフェイスコンフィギュレーションモードで **switchport mode** コマンドを使用します。モードをデバイスに適したデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

```
switchport mode {access|dynamic|{auto|desirable}|trunk}
noswitchport mode {access|dynamic|{auto|desirable}|trunk}
```

Syntax Description

access	ポートをアクセスモードに設定します（ switchport access vlan インターフェイスコンフィギュレーションコマンドの設定に応じて、スタティックアクセスまたはダイナミックアクセスのいずれか）。ポートは無条件にアクセスするように設定され、非カプセル化（タグなし）フレームを送受信する単一の非トランク VLAN インターフェイスとして動作します。アクセスポートを割り当てることができるのは、1つの VLAN だけです。
dynamic auto	ポートトランキングモードのダイナミックパラメータを auto に設定して、インターフェイスがリンクをトランクリンクに変換するように指定します。これがデフォルトのスイッチポートモードになります。
dynamic desirable	ポートトランキングモードのダイナミックパラメータを desirable に設定して、インターフェイスがリンクをトランクリンクにアクティブに変換するように指定します。
trunk	ポートは無条件にトランクに設定します。ポートはトランキング VLAN レイヤ 2 インターフェイスです。ポートは、送信元の VLAN を識別するカプセル化（タグ付き）フレームを送受信します。トランクは、2つのスイッチ間、またはスイッチとルータ間のポイントツーポイントリンクです。

Command Default

デフォルトモードは **dynamic auto** です。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

access または **trunk** キーワードによる設定が有効となるのは、**switchport mode** コマンドを使用して適切なモードでポートを設定した場合のみです。スタティックアクセスおよびトランクの設定は保存されますが、同時にアクティブにできるのはいずれかの設定だけです。

access モードを開始すると、インターフェイスは永続的な非トランキングモードになり、隣接インターフェイスがリンクから非トランクリンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを開始すると、インターフェイスは永続的なトランキング モードになり、接続先のインターフェイスがリンクからトランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

dynamic auto モードを開始すると、隣接インターフェイスが **trunk** または **desirable** モードに設定された場合に、インターフェイスはリンクをトランク リンクに変換します。

dynamic desirable モードを開始すると、隣接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定された場合に、インターフェイスはトランク インターフェイスになります。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN トランキング プロトコル (VTP) ドメインに存在する必要があります。トランク ネゴシエーションは、ポイント ツーポイント プロトコルである Dynamic Trunking Protocol (DTP) によって管理されます。ただし、一部のインターネットワーキングデバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この問題を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定し、DTP をオフにします。

- これらのリンク上でトランキングを行わない場合は、インターフェイス コンフィギュレーション モードで **switchport mode access** コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **switchport mode trunk** および **switchport nonnegotiate** コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

アクセス ポートとトランク ポートは、互いに排他的な関係にあります。

IEEE 802.1X 機能は、次の方法でスイッチポート モードに作用します。

- トランク ポートで IEEE 802.1X をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ポート設定で IEEE 802.1X を **dynamic auto** または **dynamic desirable** にイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードを **dynamic auto** または **dynamic desirable** に変更しようとしても、ポート モードは変更されません。
- ダイナミック アクセス (VLAN Query Protocol (VQP)) ポートで IEEE 802.1X をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

設定を確認するには、特権 EXEC モードで **show interfaces interface-id switchport** コマンドを入力して、*Administrative Mode* 行と *Operational Mode* 行の情報を調べます。

Examples

次の例では、ポートをアクセス モードに設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode access
```

次の例では、ポートを dynamic desirable モードに設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode dynamic desirable
```

次の例では、ポートをトランク モードに設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode trunk
```

switchport nonegotiate

ダイナミック トランキング プロトコル (DTP) ネゴシエーション パケットがレイヤ 2 インターフェイス上で送信されないように指定するには、インターフェイス コンフィギュレーション モードで **switchport nonegotiate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport nonegotiate
no switchport nonegotiate

Command Default

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

no switchport nonegotiate コマンドは nonegotiate ステータスを解除します。

このコマンドが有効なのは、インターフェイス スイッチポート モードがアクセス または トランク (**switchport mode access** または **switchport mode trunk** インターフェイス コンフィギュレーション コマンドで設定) の場合だけです。dynamic (auto または desirable) モードでこのコマンドを実行しようとすると、エラーが返されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

switchport nonegotiate コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーション パケットが送信されません。デバイスが トランキング を実行するかどうかは、**mode** パラメータ (**access** または **trunk.**) によって決まります。

- これらのリンク上で トランキング を行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキング をディセーブルにします。
- DTP をサポートしていないデバイス上の トランキング をイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスが トランク になっても DTP フレームを生成しないように設定します。

次の例では、ポートに対して トランキング モードのネゴシエーションを制限し、(モードの設定に応じて) トランク ポート または アクセス ポート として動作させる方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport nonegotiate
```

設定を確認するには、特権 EXEC モードで **show interfaces *interface-id* switchport** コマンドを入力します。

switchport voice vlan

ポートに音声 VLAN を設定するには、インターフェイス コンフィギュレーション モードで **switchport voice vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport voice vlan {vlan-id | dot1p | none | untagged | name vlan_name}
no switchport voice vlan
```

Syntax Description	
vlan-id	音声トラフィックに使用する VLAN。指定できる範囲は 1～4094 です。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。
dot1p	IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話機を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。
none	音声 VLAN に関して IP Phone に指示しません。IP Phone のキーパッドから入力された設定を使用します。
untagged	タグなしの音声トラフィックを送信するように IP Phone を設定します。これが IP Phone のデフォルト設定になります。
name vlan_name	（任意）音声トラフィックに使用する VLAN 名を指定します。最大 128 文字を入力できます。

Command Default デフォルトでは、IP Phone を自動設定しません（**none**）。
デフォルトでは、IP Phone はフレームにタグを付けません。

Command Modes インターフェイス コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines レイヤ 2 アクセス ポート上で音声 VLAN を設定する必要があります。

デバイスの Cisco IP 電話に接続しているスイッチポート上の Cisco Discovery Protocol (CDP) をイネーブルにし、Cisco IP 電話に設定情報を送信する必要があります。デフォルトでは、CDP はインターフェイス上でグローバルにイネーブルです。

VLAN ID を入力すると、IP Phone は IEEE 802.1Q フレームの音声トラフィックを指定された VLAN ID タグ付きで転送します。デバイスは IEEE 802.1Q 音声トラフィックを音声 VLAN に入れます。

dot1p、**none**、または **untagged** を選択した場合、デバイスは指定の音声トラフィックをアクセス VLAN に入れます。

すべての設定で、音声トラフィックはレイヤ 2 の IP precedence 値を運びます。音声トラフィックのデフォルトは 5 です。

音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。

アクセス VLAN で任意のポートセキュリティタイプがイネーブルにされた場合、音声 VLAN でダイナミックポートセキュリティは自動的にイネーブルになります。

音声 VLAN には、スタティックセキュア MAC アドレスを設定できません。

音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

次の例では、最初に VLAN ID と VLAN 名を対応させて、その情報を VLAN データベースに格納し、その後、アクセスモードにあるインターフェイス上の VLAN を設定します（名前を使用）。設定を確認するには、特権 EXEC コマンドで **show interfaces interface-id switchport** を入力して、Voice VLAN: 行の情報を調べます。

パート 1 - VLAN データベースに入力する

```
Device> enable
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
```

パート 2 - VLAN データベースを確認する

```
Device> enable
Device# show vlan id 55
VLAN Name Status Ports
-----
55 test active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
55 enet 100055 1500 - - - - - 0 0
Remote SPAN VLAN
-----
Disabled
Primary Secondary Type Ports
-----
```

パート 3 - VLAN 名を使用して VLAN をインターフェイスに割り当てる

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#
```

パート 4 - 設定を確認する

```
Device> enable
Device# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport voice vlan 55
switchport mode access
Switch#
```

パート 5 - インターフェイス スイッチポートでも確認できる

```
Device> enable
Device# show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

udld

単方向リンク検出 (UDLD) で、アグレッシブモードまたは通常モードをイネーブルにし、設定可能なメッセージタイマーの時間を設定するには、グローバルコンフィギュレーションモードで **udld** コマンドを使用します。すべての光ファイバポート上でアグレッシブモード UDLD または通常モード UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
udld {aggressive|enable|message time message-timer-interval}
no udld {aggressive|enable|message}
```

Syntax Description

aggressive	すべての光ファイバインターフェイスにおいて、アグレッシブモードで UDLD をイネーブルにします。
enable	すべての光ファイバインターフェイスにおいて、通常モードで UDLD をイネーブルにします。
message time <i>message-timer-interval</i>	アダプタイズメントフェーズにあり、双方向と判別されたポートにおける UDLD プロブメッセージ間の時間間隔を設定します。指定できる範囲は 1 ~ 90 秒です。デフォルトは 15 秒です。

Command Default

すべてのインターフェイスで UDLD はディセーブルです。
メッセージタイマーは 15 秒に設定されます。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

UDLD は、2つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。ノーマルモードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブモードでは、UDLD はまた、光ファイバおよびツイストペアリンクの単一方向トラフィックによる単一方向リンク、および光ファイバリンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。

プローブパケット間のメッセージ時間を変更する場合、検出速度と CPU 負荷との折り合いをつけることとなります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバインターフェイスだけです。他のインターフェイスタイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。

次のコマンドを使用して、UDLD によってシャットダウンされたインターフェイスをリセットできます。

- **udld reset** 特権 EXEC コマンド: UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション モード コマンド。
- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを入力: グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力: 指定したインターフェイスで UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval interval** グローバル コンフィギュレーション コマンド: 自動的に UDLD error-disabled ステートから回復します。

次の例では、すべての光ファイバインターフェイスで UDLD をイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# udld enable
```

設定を確認するには、特権 EXEC モードで **show udld** コマンドを入力します。

udld port

個々のインターフェイスで単方向リンク検出 (UDLD) をイネーブルにするか、または光ファイバインターフェイスがグローバルコンフィギュレーションモードの **udld** コマンドによってイネーブルになるのを防ぐには、インターフェイス コンフィギュレーション モードで **udld port** コマンドを使用します。グローバル コンフィギュレーション モードの **udld** コマンドの設定に戻るか、または非光ファイバポートで入力された場合に UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。

udld port [aggressive]
no udld port [aggressive]

Syntax Description	aggressive (任意) 指定されたインターフェイスにおいて、アグレッシブモードでUDLDをイネーブルにします。				
Command Default	光ファイバインターフェイスでは、UDLDはディセーブルになっていますが、光ファイバインターフェイスは、グローバルコンフィギュレーションモードの udld enable または udld aggressive コマンドのステートに応じて UDLD をイネーブルにします。 非光ファイバインターフェイスでは、UDLD はディセーブルです。				
Command Modes	インターフェイス コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	<p>UDLD 対応ポートが別のデバイスの UDLD 非対応ポートに接続されている場合、このポートは単方向リンクを検出できません。</p> <p>UDLD は、2つの動作モードをサポートしています。通常 (デフォルト) とアグレッシブです。ノーマルモードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単方向リンクを検出します。アグレッシブモードでは、UDLD はまた、光ファイバおよびツイストペアリンクの単方向トラフィックによる単方向リンク、および光ファイバリンクにおいて誤って接続されたインターフェイスによる単方向リンクを検出します。</p> <p>UDLD を通常モードでイネーブルにするには、インターフェイス コンフィギュレーションモードで udld port コマンドを使用します。UDLD をアグレッシブモードでイネーブルにするには、インターフェイス コンフィギュレーションモードで udld port aggressive コマンドを使用します。</p> <p>UDLD の制御を udld enable グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで no udld port コマンドを使用します。</p>				

グローバル コンフィギュレーション モードの **udld enable** または **udld aggressive** コマンドの設定を上書きする場合は、光ファイバポートで **udld port aggressive** コマンドを使用します。この設定を削除して UDLD イネーブル化の制御をグローバル コンフィギュレーション モードの **udld** コマンドに戻したり、UDLD を非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで **no** 形式を使用します。

次のコマンドを使用して、UDLD によってシャットダウンされたインターフェイスをリセットできます。

- 特権 EXEC モードの **udld reset** コマンド: UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- インターフェイス コンフィギュレーション モードの **shutdown** および **no shutdown** コマンド。
- グローバル コンフィギュレーション モードの **no udld enable** コマンドの後にグローバル コンフィギュレーション モードで **udld {aggressive | enable}** コマンドを入力: グローバルに UDLD を再度イネーブルにします。
- インターフェイス コンフィギュレーション モードの **no udld port** コマンドの後にインターフェイス コンフィギュレーション モードで **udld port** または **udld port aggressive** コマンドを入力: 指定したインターフェイスで UDLD を再度イネーブルにします。
- グローバル コンフィギュレーション モードの **errdisable recovery cause udld** および **errdisable recovery interval interval** コマンド: 自動的に UDLD error-disabled ステートから回復します。

次の例では、ポート上で UDLD をイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port
```

次の例では、グローバル コンフィギュレーション モードの **udld** コマンドの設定に関係なく、光ファイバインターフェイス上で UDLD をディセーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# no udld port
```

設定を確認するには、特権 EXEC モードで **show running-config** または **show udld interface** コマンドを入力します。

udld reset

単方向リンク検出 (UDLD) によりディセーブルにされたインターフェイスをすべてリセットし、インターフェイスのトラフィックを再開させるには、特権 EXEC モードで **udld reset** コマンドを使用します (イネーブルの場合には、スパニングツリー、ポート集約プロトコル (PAgP)、ダイナミック トランッキング プロトコル (DTP) などの他の機能を介することで有効になります)。

udld reset

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

インターフェイスの設定で、UDLD がまだイネーブルである場合、これらのポートは再び UDLD の稼働を開始し、問題が修正されていない場合には同じ理由でディセーブルになります。

次の例では、UDLD によってディセーブルにされたすべてのインターフェイスをリセットする方法を示します。

```
Device> enable
Device# udld reset
1 ports shutdown by UDLD were reset.
```

vlan dot1q tag native

すべての IEEE 802.1Q トランクポートでネイティブ VLAN フレームのタグングをイネーブルにするには、グローバル コンフィギュレーション モードで **vlan dot1q tag native** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vlan dot1q tag native
no vlan dot1q tag native

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IEEE 802.1Q ネイティブ VLAN タグングはディセーブルです。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

Usage Guidelines

イネーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされます。

ディセーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされません。

このコマンドを IEEE 802.1Q トンネリング機能とともに使用できます。この機能は、サービス プロバイダ ネットワークのエッジデバイスで動作し、VLAN 内 VLAN 階層構造を使用し、タグ付きパケットをタグ付けして VLAN スペースを拡張します。サービス プロバイダー ネットワークへのパケット送信に IEEE 802.1Q トランク ポートを使用する必要があります。ただし、サービス プロバイダー ネットワークのコアを通過するパケットも IEEE 802.1Q トランクで伝送される可能性があります。IEEE 802.1Q トランクのネイティブ VLAN が同一デバイス上のトンネリングポートのネイティブ VLAN と一致する場合は、ネイティブ VLAN 上のトラフィックは送信トランクポートでタグ付けされません。このコマンドは、すべての IEEE 802.1Q トランク ポート上のネイティブ VLAN パケットが確実にタグ付けされるようにします。

IEEE 802.1Q トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、ネイティブ VLAN フレームの IEEE 802.1Q タグングをイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# vlan dot1q tag native
Device(config)# end
```

設定を確認するには、**show vlan dot1q tag native** 特権 EXEC コマンドを入力します。



PART VII

ネットワーク管理

- [ネットワーク管理コマンド, on page 957](#)



ネットワーク管理コマンド

- [cache](#), on page 960
- [clear flow exporter](#), on page 963
- [clear flow monitor](#), on page 964
- [clear snmp stats hosts](#), on page 966
- [collect](#), on page 967
- [collect counter](#), on page 969
- [collect flow sampler](#), on page 970
- [collect interface](#), on page 971
- [collect ipv4 destination](#), on page 972
- [collect ipv4 source](#), on page 973
- [collect timestamp absolute](#), on page 975
- [collect transport tcp flags](#), on page 976
- [collect routing next-hop address](#), on page 977
- [datalink flow monitor](#), on page 978
- [debug flow exporter](#), on page 979
- [debug flow monitor](#), on page 980
- [debug flow record](#), on page 981
- [debug sampler](#), on page 982
- [description](#), on page 983
- [destination](#), on page 984
- [dscp](#), on page 986
- [event manager applet](#), on page 987
- [export-protocol netflow-v9](#), on page 991
- [export-protocol netflow-v5](#), on page 992
- [exporter](#), on page 993
- [fconfigure](#), on page 994
- [flow exporter](#), on page 995
- [flow monitor](#), on page 996
- [flow record](#), on page 997
- [ip wccp](#), on page 998
- [ip flow monitor](#), on page 1000
- [ipv6 flow monitor](#), on page 1002
- [ipv6 deny echo reply](#), on page 1004

- match datalink dot1q priority, on page 1005
- match datalink dot1q vlan, on page 1006
- match datalink ethertype, on page 1007
- match datalink mac, on page 1008
- match datalink vlan, on page 1010
- match flow cts, on page 1011
- match flow direction, on page 1012
- match interface, on page 1013
- match ipv4, on page 1014
- match ipv4 destination address, on page 1015
- match ipv4 source address, on page 1016
- match ipv4 ttl, on page 1017
- match ipv6, on page 1018
- match ipv6 destination address, on page 1019
- match ipv6 hop-limit, on page 1020
- match ipv6 source address, on page 1021
- map platform-type, on page 1022
- match transport, on page 1023
- match transport icmp ipv4, on page 1024
- match transport icmp ipv6, on page 1025
- match platform-type, on page 1026
- mode random 1 out-of, on page 1027
- monitor capture (interface/control plane), on page 1028
- monitor capture buffer, on page 1030
- monitor capture export, on page 1031
- monitor capture limit, on page 1032
- monitor capture start, on page 1033
- monitor capture stop, on page 1034
- monitor session destination, on page 1035
- monitor session filter, on page 1039
- monitor session source, on page 1041
- option, on page 1044
- record, on page 1046
- sampler, on page 1047
- show class-map type control subscriber, on page 1048
- show ip sla statistics, on page 1049
- show monitor, on page 1051
- show monitor capture, on page 1053
- show parameter-map type subscriber attribute-to-service, on page 1055
- show platform software fed switch ip wccp, on page 1056
- show platform software swspan , on page 1058
- show flow exporter, on page 1060
- show flow interface, on page 1062
- show flow monitor, on page 1064
- show flow record, on page 1069
- show sampler, on page 1070

- [show snmp stats](#), on page 1072
- [snmp ifmib ifindex persist](#), on page 1074
- [snmp-server community](#), on page 1075
- [snmp-server enable traps](#), on page 1077
- [snmp-server enable traps bridge](#), on page 1081
- [snmp-server enable traps bulkstat](#), on page 1082
- [snmp-server enable traps call-home](#), on page 1083
- [snmp-server enable traps cef](#), on page 1084
- [snmp-server enable traps envmon](#), on page 1085
- [snmp-server enable traps errdisable](#), on page 1086
- [snmp-server enable traps flash](#), on page 1087
- [snmp-server enable traps isis](#), on page 1088
- [snmp-server enable traps license](#), on page 1089
- [snmp-server enable traps mac-notification](#), on page 1090
- [snmp-server enable traps ospf](#), on page 1091
- [snmp-server enable traps pim](#), on page 1093
- [snmp-server enable traps port-security](#), on page 1094
- [snmp-server enable traps power-ethernet](#), on page 1095
- [snmp-server enable traps snmp](#), on page 1096
- [snmp-server enable traps storm-control](#), on page 1097
- [snmp-server enable traps stpx](#), on page 1098
- [snmp-server enable traps transceiver](#), on page 1099
- [snmp-server enable traps vrfmib](#), on page 1100
- [snmp-server enable traps vstack](#), on page 1101
- [snmp-server engineID](#), on page 1102
- [snmp-server group](#), on page 1103
- [snmp-server host](#), on page 1107
- [snmp-server manager](#), on page 1112
- [snmp-server user](#), on page 1113
- [snmp-server view](#), on page 1118
- [source](#), on page 1120
- [socket](#), on page 1122
- [switchport mode access](#), on page 1123
- [switchport voice vlan](#), on page 1124
- [ttl](#), on page 1125
- [transport](#), on page 1126
- [template data timeout](#), on page 1127
- [udp peek](#), on page 1128

cache

フローモニタのフローキャッシュパラメータを設定するには、フロー モニタ コンフィギュレーション モードで **cache** コマンドを使用します。フローモニタのフローキャッシュパラメータを削除するには、このコマンドの **no** 形式を使用します。

```
cache {timeout {active|inactive|update} seconds|type normal}
no cache {timeout {active|inactive|update} |type}
```

Syntax Description

timeout	フロー タイムアウトを指定します。
active	アクティブ フロー タイムアウトを指定します。
inactive	非アクティブ フロー タイムアウトを指定します。
update	永久フローキャッシュの更新タイムアウトを指定します。
<i>seconds</i>	タイムアウト値（秒単位）。通常のフローキャッシュの場合、指定できる範囲は30~604800（7日）です。永久フローキャッシュの場合は、指定できる範囲は1~604800（7日）です。
type	フローキャッシュのタイプを指定します。
normal	通常キャッシュタイプを設定します。フローキャッシュ内のエントリは、 timeout active seconds および timeout inactive seconds の設定に従って期限切れになります。これがデフォルトのキャッシュタイプです。

Command Default

デフォルトのフロー モニタ フロー キャッシュ パラメータが使用されます。
フローモニタの以下のフロー キャッシュ パラメータがイネーブルになっています。

- キャッシュタイプ: normal
- アクティブ フロー タイムアウト: 1800 秒

Command Modes

フロー モニタ コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

各フローモニタには、モニタするすべてのフローの保存に使用するキャッシュがあります。各キャッシュには、フローがキャッシュ内に留まることができる時間など、設定可能な要素があります。フローがタイムアウトするとキャッシュから削除され、対応するフローモニタ用に設定されている任意のエクスポートに送信されます。

cache timeout active コマンドでは、通常タイプのキャッシュのエージング動作を制御します。フローが長時間アクティブになっている場合、通常はエージアウト（そのフローの後続の packets 用の新しいフローを開始）することが望まれます。このエージアウトプロセスを行うことで、エクスポートを受信するモニタリングアプリケーションに最新の情報を反映し続けることができます。デフォルトでは、このタイムアウトは1800秒（30分）ですが、システム要件に応じて調整できます。大きい値を設定すると、存続時間の長いフローを単一のフローレコードに記録することができます。小さい値を設定すると、存続時間の長い新しいフローが開始されてから、そのフローのデータがエクスポートされるまでの遅延が短縮されます。アクティブフロータイムアウトを変更した場合、新しいタイムアウト値はただちに有効になります。

また、**cache timeout inactive** コマンドでも、通常タイプのキャッシュのエージング動作を制御できます。指定した時間内にフローでアクティビティが検出されない場合、そのフローはエージアウトされます。デフォルトでは、このタイムアウトは15秒ですが、この値は想定されるトラフィックのタイプに応じて調整できます。存続時間の短いフローが多数存在し、多くのキャッシュエントリが消費されている場合は、非アクティブタイムアウトを短縮することでこのオーバーヘッドを削減できます。多数のフローが、データを収集し終わる前に頻繁にエージアウトしている場合は、このタイムアウトを延長することでフローの相関関係を向上できます。非アクティブフロータイムアウトを変更した場合、新しいタイムアウト値はただちに有効になります。

cache timeout update コマンドでは、永久タイプのキャッシュによって送信される定期的なアップデートを制御します。この動作は、アクティブタイムアウトの動作に類似しています。ただし、この動作によって、キャッシュからキャッシュエントリは削除されません。デフォルトでは、このタイマー値は1800秒（30分）です。

cache type normal コマンドでは、通常キャッシュタイプを指定します。これがデフォルトのキャッシュタイプです。キャッシュのエントリは、**timeout active seconds** および **timeout inactive seconds** の設定に従って、エージアウトされます。キャッシュエントリはエージアウトされると、キャッシュから削除され、そのキャッシュに対応するモニタ用に設定されているエクスポートによってエクスポートされます。

キャッシュをデフォルト設定に戻すには、**default cache** フローモニタ コンフィギュレーション コマンドを使用します。



Note キャッシュが一杯になると、新しいフローはモニタされません。

次に、フローモニタキャッシュのアクティブタイムアウトを設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout active 4800
```

次に、フローモニタキャッシュの非アクティブタイマーを設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout inactive 30
```

次に、永久キャッシュのアップデートタイムアウトを設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1  
Device(config-flow-monitor)# cache timeout update 5000
```

次に、通常キャッシュを設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1  
Device(config-flow-monitor)# cache type normal
```

clear flow exporter

Flexible Netflow フローエクスポートの統計情報をクリアするには、特権 EXEC モードで **clear flow exporter** コマンドを使用します。

```
clear flow exporter [[name] exporter-name] statistics
```

Syntax Description

name	(任意) フローエクスポートの名前を指定します。
<i>exporter-name</i>	(任意) 以前に設定されたフローエクスポートの名前。
statistics	フローエクスポートの統計情報をクリアします。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear flow exporter コマンドは、フローエクスポートからすべての統計情報を削除します。これらの統計情報はエクスポートされず、キャッシュ内に保存されていたデータは失われます。

show flow exporter statistics 特権 EXEC コマンドを使用して、フローエクスポートの統計情報を表示できます。

Examples

次の例では、デバイスで設定されているすべてのフローエクスポートの統計情報をクリアします。

```
Device# clear flow exporter statistics
```

次の例では、FLOW-EXPORTER-1 という名前のフローエクスポートの統計情報をクリアします。

```
Device# clear flow exporter FLOW-EXPORTER-1 statistics
```

clear flow monitor

フローモニタキャッシュまたはフローモニタ統計情報をクリアし、フローモニタキャッシュ内のデータを強制的にエクスポートするには、特権 EXEC モードで **clear flow monitor** コマンドを使用します。

clear flow monitor [**name**] *monitor-name* [[**cache**] **force-export** | **statistics**]

Syntax Description

name	フローモニタの名前を指定します。
<i>monitor-name</i>	以前に設定されたフローモニタの名前
cache	(任意) フローモニタキャッシュ情報をクリアします。
force-export	(任意) フローモニタキャッシュ統計情報を強制的にエクスポートします。
statistics	(任意) フローモニタの統計情報をクリアします。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

clear flow monitor cache コマンドを実行すると、フローモニタキャッシュからすべてのエントリが削除されます。キャッシュ内のエントリはエクスポートされ、キャッシュ内に保存されていたデータは失われます。



Note クリアされたキャッシュエントリの統計情報は保持されます。

clear flow monitor force-export コマンドを実行すると、フローモニタキャッシュからすべてのエントリが削除され、それらのエントリはフローモニタに割り当てられているすべてのフローエクスポートを使用してエクスポートされます。このアクションにより、CPU 使用率は一時的に増加します。このコマンドの使用には注意が必要です。

clear flow monitor statistics コマンドを実行すると、このフローモニタの統計情報がクリアされます。



Note **clear flow monitor statistics** コマンドを実行しても、現在のエントリに関する統計情報はクリアされません。なぜなら、この情報はキャッシュ内に保存されているエントリ数のインジケータであり、キャッシュは、このコマンドによってクリアされないためです。

フローモニタの統計情報を表示するには、**show flow monitor statistics** 特権 EXEC コマンドを使用します。

Examples

次に、FLOW-MONITOR-1 という名前のフローモニタの統計情報とキャッシュエントリをクリアする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1
```

次に、FLOW-MONITOR-1 という名前のフローモニタの統計情報とキャッシュエントリをクリアして、強制的にエクスポートする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 force-export
```

次に、FLOW-MONITOR-1 という名前のフローモニタのキャッシュをクリアして、強制的にエクスポートする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 cache force-export
```

次に、FLOW-MONITOR-1 という名前のフローモニタの統計情報をクリアする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 statistics
```

clear snmp stats hosts

NMS の IP アドレス、NMS がエージェントをポーリングした回数、およびポーリングのタイムスタンプをクリアするには、特権 EXEC モードで **clear snmp stats hosts** コマンドを使用します。

clear snmp stats hosts

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default SNMP エージェントにポーリングされた SNMP マネージャの詳細がシステムに保存されます。

Command Modes 特権 EXEC (#)

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines **clear snmp stats hosts** コマンドは、SNMP エージェントにポーリングされたすべてのエントリを削除するために使用します。

次に、**clear snmp stats hosts** コマンドの出力例を示します。

```
Device# clear snmp stats hosts
Request Count                               Last Timestamp                               Address
```

collect

フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドへの値の取り込みを有効にするには、フローレコードコンフィギュレーションモードで **collect** コマンドを使用します。

collect {counter | interface | timestamp | transport}

Syntax Description

counter	フローレコードの非キーフィールドとしてフロー内のバイト数またはパケット数を設定します。詳細については、 <i>collect counter</i> を参照してください。
interface	入力および出力インターフェイス名をフローレコードの非キーフィールドとして設定します。詳細については、 <i>collect interface</i> を参照してください。
timestamp	フロー内の最初または最後に確認されたパケットの絶対時間をフローレコードの非キーフィールドとして設定します。詳細については、 <i>collect timestamp absolute</i> を参照してください。
transport	フローレコードからの転送 TCP フラグの収集を有効にします。詳細については、 <i>collect transport tcp flags</i> を参照してください。

Command Default

フローモニタレコードの非キーフィールドは設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。



Note **flowusername** キーワードは、コマンドラインのヘルプストリングには表示されますが、サポートされていません。

次に、フローの合計バイト数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1  
Device(config-flow-record)# collect counter bytes long
```

collect counter

フローレコードの非キーフィールドとしてフロー内のバイト数またはパケット数を設定するには、フローレコードコンフィギュレーションモードで **collect counter** コマンドを使用します。フロー（カウンタ）内のバイト数またはパケット数をフローレコードの非キーフィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
collect counter {bytes layer2 long | bytes long | packets long}
no collect counter {bytes layer2 long | bytes long | packets long}
```

Syntax Description

bytes layer2 long	フローで確認されるレイヤ2のバイト数を非キーフィールドとして設定し、64ビットカウンタを使用してフローからレイヤ2の合計バイト数を収集します。
bytes long	フローで確認されるバイト数を非キーフィールドとして設定し、64ビットカウンタを使用してフローから合計バイト数を収集します。
packets long	フローで確認されるパケット数を非キーフィールドとして設定し、64ビットカウンタを使用してフローから合計パケット数を収集します。

Command Default

フロー内のバイト数またはパケット数は、非キーフィールドとして設定されません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

collect counter bytes long コマンドは、フローで確認されるバイト数の64ビットカウンタを設定します。

collect counter packets long コマンドは、フローでパケットが確認されるたびに増分される64ビットのカウンタを設定します。64ビットのカウンタが0に戻って再びカウントを開始することはまず考えられません。

このコマンドをデフォルト設定に戻すには、**no collect counter** または **default collect counter** フローレコードコンフィギュレーションコマンドを使用します。

次に、フローの合計バイト数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

次に、フローからの合計パケット数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

collect flow sampler

フローサンプラー ID をレコードの非キーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **collect flow sampler** コマンドを使用します。フローレコードの非キーフィールドとしてフローサンプラー ID を使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

collect flow sampler
no collect flow sampler

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

フローサンプラーは、非キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション (config-flow-record)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

Usage Guidelines

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

collect flow sampler コマンドは、異なるサンプリングレートで複数のフローサンプラーを使用している場合に効果を発揮します。非キーフィールドには、フローのモニタに使用されるフローサンプラーの ID が含まれます。

Examples

次に、非キーフィールドとしてフローに割り当てられているフローサンプラーの ID を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect flow sampler
```

Related Commands

コマンド	説明
flow exporter	フローエクスポートを作成します。
flow record	Flexible NetFlow のフローレコードを作成します。

collect interface

フローレコードの非キーフィールドとして入力および出力インターフェイス名を設定するには、フローレコードコンフィギュレーションモードで **collect interface** コマンドを使用します。入力および出力インターフェイスをフローレコードの非キーフィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
collect interface {input | output}
no collect interface {input | output}
```

Syntax Description

input 入力インターフェイス名を非キーフィールドとして設定し、フローから入力インターフェイスを収集します。

output 出力インターフェイス名を非キーフィールドとして設定し、フローから出力インターフェイスを収集します。

Command Default

入力および出力インターフェイス名は非キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Flexible NetFlow **collect** コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

このコマンドをデフォルト設定に戻すには、**no collect interface** または **default collect interface** フローレコードコンフィギュレーションコマンドを使用します。

次の例では、非キーフィールドとして出力インターフェイスを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect interface output
```

次の例では、非キーフィールドとして入力インターフェイスを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect interface input
```

collect ipv4 destination

IPv4 宛先をフローレコードの非キーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **collect ipv4 destination** コマンドを使用します。フローレコードの非キーフィールドとして IPv4 宛先フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
collect ipv4 destination {mask|prefix} [minimum-mask mask]
no collect ipv4 destination {mask|prefix} [minimum-mask mask]
```

Syntax Description

mask	IPv4 宛先マスクを非キーフィールドとして設定し、IPv4 宛先マスクの値をフローから収集できるようにします。
prefix	IPv4 宛先のプレフィックスを非キーフィールドとして設定し、IPv4 宛先のプレフィックスの値をフローから収集できるようにします。
minimum-mask mask	(任意) 最小マスクのサイズをビット単位で指定します。範囲: 1 ~ 32。

Command Default

IPv4 宛先は非キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション (config-flow-record)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

Usage Guidelines

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

Examples

次に、プレフィックスが 16 ビットのフローから IPv4 宛先プレフィックスを非キーフィールドとして設定する例を示します。

```
Device> enable
Device> configure terminal
Device (config)# flow record FLOW-RECORD-1
Device (config-flow-record)# collect ipv4 destination prefix minimum-mask 16
```

Related Commands

コマンド	説明
flow record	Flexible NetFlow のフローレコードを作成します。

collect ipv4 source

IPv4送信元をフローレコードの非キーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **collect ipv4 source** コマンドを使用します。フローレコードの非キーフィールドとして IPv4送信元フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
collect ipv4 source {mask|prefix} [minimum-mask mask]
no collect ipv4 source {mask|prefix} [minimum-mask mask]
```

Syntax Description

mask	IPv4送信元のマスクを非キーフィールドとして設定し、IPv4送信元マスクの値をフローから収集できるようにします。
prefix	IPv4送信元のプレフィックスを非キーフィールドとして設定し、フローから IPv4送信元プレフィックスの値を収集できるようにします。
minimum-mask mask	(任意) 最小マスクのサイズをビット単位で指定します。範囲: 1 ~ 32。

Command Default

IPv4送信元フィールドは非キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション (config-flow-record)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

Usage Guidelines

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

collect ipv4 source prefix minimum-mask

送信元プレフィックスは、IPv4送信元のネットワーク部分です。オプションの最小マスクを使用すると、大規模ネットワークに関する多くの情報を収集できます。

collect ipv4 source mask minimum-mask

送信元マスクは、送信元のネットワーク部分を構成するビット数です。オプションの最小マスクでは、最小値を設定できます。このコマンドは、送信元プレフィックスフィールドに設定された最小マスクがあり、そのマスクがプレフィックスで使用される場合に役立ちます。この場合、最小マスクに設定されている値は、プレフィックスフィールドとマスクフィールドで同じである必要があります。

また、コレクタがプレフィックスフィールドの最小マスク設定を認識している場合は、最小マスクなしでマスクフィールドを設定して、実際のマスクとプレフィックスを計算できます。

Examples

次に、プレフィックスが16ビットのフローからIPv4送信元プレフィックスを非キーフィールドとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect ipv4 source prefix minimum-mask 16
```

Related Commands

コマンド	説明
flow record	Flexible NetFlow のフローレコードを作成します。

collect timestamp absolute

フロー内の最初または最後に確認されたパケットの絶対時間をフローレコードの非キーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **collect timestamp absolute** コマンドを使用します。フロー内の最初または最後に確認されたパケットをフローレコードの非キーフィールドとして使用するのを無効にするには、このコマンドの **no** 形式を使用します。

```
collect timestamp absolute {first|last}
no collect timestamp absolute {first|last}
```

Syntax Description

first フロー内の最初に確認されたパケットの絶対時間を非キーフィールドとして設定し、フローからのタイムスタンプの収集を有効にします。

last フロー内の最後に確認されたパケットの絶対時間を非キーフィールドとして設定し、フローからのタイムスタンプの収集を有効にします。

Command Default

絶対時間フィールドは非キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
------	------

Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
--------------------------	-----------------

Usage Guidelines

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

次に、フロー内の最初に確認されたパケットの絶対時間に基づくタイムスタンプを非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute first
```

次に、フロー内の最後に確認されたパケットの絶対時間に基づくタイムスタンプを非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute last
```

collect transport tcp flags

フローからの転送 TCP フラグの収集をイネーブルにするには、フローレコードコンフィギュレーションモードで **collect transport tcp flags** コマンドを使用します。フローからの転送 TCP フラグの収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

collect transport tcp flags
no collect transport tcp flags

Syntax Description	このコマンドには引数またはキーワードはありません。				
Command Default	トランスポート層フィールドは非キーフィールドとして設定されていません。				
Command Modes	フローレコードコンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	トランスポート層フィールドの値は、フロー内のすべてのパケットから取得されます。収集する TCP フラグを指定することはできません。転送 TCP フラグの収集のみ指定できます。すべての TCP フラグはこのコマンドで収集されます。次の転送 TCP フラグを収集します。				

- **ack:** TCP 確認応答フラグ
- **cwr:** TCP 輻輳ウィンドウ縮小フラグ
- **ece:** TCP ECN エコーフラグ
- **fin:** TCP 終了フラグ
- **psh:** TCP プッシュフラグ
- **rst:** TCP リセットフラグ
- **syn:** TCP 同期フラグ
- **urg:** TCP 緊急フラグ

このコマンドをデフォルト設定に戻すには、**no collect collect transport tcp flags** または **default collect collect transport tcp flags** フローレコードコンフィギュレーションコマンドを使用します。

次に、フローから TCP フラグを収集する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect transport tcp flags
```

collect routing next-hop address

ネクストホップアドレス値を非キーフィールドとして設定し、フローからネクストホップ情報を収集するには、フローレコードコンフィギュレーションモードで **collect routing next-hop address** コマンドを使用します。フローレコードの非キーフィールドとして1つ以上のルーティング属性を使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

collect routing next-hop address ipv4
no collect routing next-hop address ipv4

Syntax Description

ipv4	ネクストホップアドレス値が IPv4 アドレスであることを指定します。
-------------	-------------------------------------

Command Default

ネクストホップアドレス値が非キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション (config-flow-record)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

Usage Guidelines

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

Examples

次に、ネクストホップアドレスを非キーフィールドとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect routing next-hop address ipv4
```

Related Commands

コマンド	説明
flow record	フローレコードを作成し、Flexible NetFlow フローレコードコンフィギュレーションモードを開始します。

datalink flow monitor

インターフェイスに Flexible NetFlow フローモニタを適用するには、インターフェイス コンフィギュレーションモードで **datalink flow monitor** コマンドを使用します。Flexible NetFlow フローモニタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
datalink flow monitor monitor-name {input | output | sampler sampler-name}
no datalink flow monitor monitor-name {input | output | sampler sampler-name}
```

Syntax Description

<i>monitor-name</i>	インターフェイスに適用するフロー モニタの名前。
sampler <i>sampler-name</i>	フロー モニタ用に指定したフロー サンプラーをイネーブルにします。
input	スイッチがインターフェイスで受信するトラフィックをモニタします。
output	スイッチがインターフェイスで送信するトラフィックをモニタします。

Command Default

フローモニタはイネーブルになっていません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

datalink flow monitor コマンドを使用してインターフェイスにフローモニタを適用する前に、**flow monitor** グローバルコンフィギュレーションコマンドを使用してフローモニタを作成し、**sampler** グローバルコンフィギュレーションコマンドを使用してフローサンプラーを作成しておく必要があります。

フローモニタ用のフローサンプラーをイネーブルにするには、事前にサンプラーを作成しておく必要があります。



Note **datalink flow monitor** コマンドは、非 IPv4 および非 IPv6 トラフィックだけをモニタします。IPv4 トラフィックをモニタするには、**ip flow monitor** コマンドを使用します。IPv6 トラフィックをモニタするには、**ipv6 flow monitor** コマンドを使用します。

次に、インターフェイス上での Flexible NetFlow データリンク モニタリングをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# datalink flow monitor FLOW-MONITOR-1 sampler FLOW-SAMPLER-1 input
```

debug flow exporter

Flexible NetFlow フローエクスポートのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug flow exporter** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug flow exporter [[name] exporter-name] [error | event | packets number]
no debug flow exporter [[name] exporter-name] [error | event | packets number]
```

Syntax Description

name	(任意) フローエクスポートの名前を指定します。
exporter-name	(任意) 前に設定されたフローエクスポートの名前。
error	(任意) フローエクスポートのエラーのデバッグをイネーブルにします。
event	(任意) フローエクスポートのイベントのデバッグをイネーブルにします。
packets	(任意) フローエクスポートのパケットレベルのデバッグをイネーブルにします。
number	(任意) フローエクスポートのパケットレベルのデバッグでデバッグするパケット数。指定できる範囲は 1 ~ 65535 です。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の例は、フローエクスポートのパケットがプロセス送信用のキューに格納されたことを示しています。

```
Device# debug flow exporter
May 21 21:29:12.603: FLOW EXP: Packet queued for process send
```

debug flow monitor

Flexible NetFlow フローモニタのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug flow monitor** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug flow monitor [error|[name] monitor-name [cache [error]|error|packets packets]]
no debug flow monitor [error|[name] monitor-name [cache [error]|error|packets packets]]
```

Syntax Description

error	(任意) すべてのフロー モニタまたは指定されたフロー モニタのフロー モニタ エラーのデバッグをイネーブルにします。
name	(任意) フロー モニタの名前を指定します。
monitor-name	(任意) 事前に設定されたフロー モニタの名前。
cache	(任意) フロー モニタ キャッシュのデバッグをイネーブルにします。
cache error	(任意) フロー モニタ キャッシュ エラーのデバッグをイネーブルにします。
packets	(任意) フロー モニタのパケットレベルのデバッグをイネーブルにします。
パケット	(任意) フロー モニタのパケットレベルのデバッグでデバッグするパケットの数。指定できる範囲は 1 ~ 65535 です。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の例は、FLOW-MONITOR-1 のキャッシュが削除されたことを示しています。

```
Device# debug flow monitor FLOW-MONITOR-1 cache
May 21 21:53:02.839: FLOW MON: 'FLOW-MONITOR-1' deleted cache
```

debug flow record

Flexible NetFlow フローレコードのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug flow record** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug flow record [[name] record-name | options {sampler-table} | [detailed | error]]
no debug flow record [[name] record-name | options {sampler-table} | [detailed | error]]
```

Syntax Description

name	(任意) フローレコードの名前を指定します。
record-name	(任意) 前に設定されたユーザ定義のフローレコードの名前。
options	(任意) 他のフローレコードオプションに関する情報が含まれます。
sampler-table	(任意) サンプラーテーブルに関する情報が含まれます。
detailed	(任意) 詳細情報を表示します。
error	(任意) エラーのみを表示します。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、フローレコードのデバッグを有効にする例を示します。

```
Device# debug flow record FLOW-record-1
```

debug sampler

Flexible NetFlow サンプラーのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug sampler** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug sampler [detailed | error | [name] sampler-name [detailed | error | sampling samples]]
no debug sampler [detailed | error | [name] sampler-name [detailed | error | sampling]]
```

Syntax Description

detailed	(任意) サンプラー要素の詳細デバッグをイネーブルにします。
error	(任意) サンプラー エラーのデバッグをイネーブルにします。
name	(任意) サンプラーの名前を指定します。
<i>sampler-name</i>	(任意) 前に設定されたサンプラーの名前。
sampling samples	(任意) サンプリングのデバッグをイネーブルにし、デバッグするサンプルの数を指定します。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、デバッグプロセスが SAMPLER-1 というサンプラーの ID を取得した場合の出力例を示します。

```
Device# debug sampler detailed
*May 28 04:14:30.883: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et1/0,0)
get ID succeeded:1
*May 28 04:14:30.971: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et0/0,I)
get ID succeeded:1
```

description

フロー モニタ、フロー エクスポート、またはフロー レコードの説明を設定するには、該当するコンフィギュレーションモードで **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *description*
no description *description*

Syntax Description

description フロー モニタ、フロー エクスポート、またはフロー レコードを説明するテキスト文字列。

Command Default

フロー サンプラー、フロー モニタ、フロー エクスポート、またはフロー レコードのデフォルトの説明は「ユーザ定義」です。

Command Modes

次のコマンドモードがサポートされています。

フロー エクスポート コンフィギュレーション

フロー モニタ コンフィギュレーション

フロー レコード コンフィギュレーション

Command History

リリース	変更内容
------	------

Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
--------------------------	-----------------

Usage Guidelines

このコマンドをデフォルト設定に戻すには、該当するコンフィギュレーションモードで **no description** または **default description** コマンドを使用します。

次に、フロー モニタの説明を設定する例を示します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

destination

フローエクスポートのエクスポート宛先を設定するには、フローエクスポート コンフィギュレーション モードで **destination** コマンドを使用します。フローエクスポートのエクスポート宛先を削除するには、このコマンドの **no** 形式を使用します。

```
destination {hostnameip-address} vrf vrf-label
no destination {hostnameip-address} vrf vrf-label
```

Syntax Description

<i>hostname</i>	NetFlow 情報を送信するデバイスのホスト名。
<i>ip-address</i>	NetFlow 情報を送信するワークステーションの IPv4 アドレス。
vrf	(任意) エクスポート データ パケットをグローバル ルーティング テーブルではなく、名前付きバーチャルプライベートネットワーク (VPN) ルーティングおよび転送 (VRF) インスタンスに送信して、宛先にルーティングするように指定します。
<i>vrf-label</i>	VRF インスタンスの名前。

Command Default

エクスポート宛先は設定されていません。

Command Modes

フローエクスポート コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

各フローエクスポートには、宛先アドレスまたはホスト名を 1 つのみ指定できます。

デバイスの IP アドレスの代わりに、ホスト名を設定すると、ホスト名は直ちに解決され、IPv4 アドレスが実行コンフィギュレーションに保存されます。ドメインネームシステム (DNS) の最初の名前解決に使用されたホスト名と IP アドレスのマッピングが DNS サーバ上で動的に変わる場合は、デバイスでこれが検出されないため、エクスポートされたデータは最初の IP アドレスに送信され続け、データは失われます。

このコマンドをデフォルト設定に戻すには、フローエクスポート コンフィギュレーション モードで **no destination** または **default destination** コマンドを使用します。

次の例に、宛先システムに Flexible NetFlow キャッシュエントリをエクスポートするようにネットワークデバイスを設定する方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

次の例に、VRF-1 という名前の VRF を使用して宛先システムに Flexible NetFlow キャッシュエントリをエクスポートするようにネットワーク デバイスを設定する方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 172.16.0.2 vrf VRF-1
```

dscp

フローエクスポート データグラムの Differentiated Services Code Point (DSCP; DiffServ コードポイント) の値を設定するには、フローエクスポート コンフィギュレーション モードで **dscp** コマンドを使用します。フローエクスポート データグラムの DSCP 値を削除するには、このコマンドの **no** 形式を使用します。

```
dscp dscp
no dscp dscp
```

Syntax Description	<i>dscp</i> エクスポートされたデータグラムの DSCP フィールドで使用される DSCP。指定できる範囲は 0 ～ 63 です。デフォルトは 0 です。				
Command Default	Differentiated Services Code Point (DSCP; DiffServ コードポイント) 値は 0 です。				
Command Modes	フローエクスポート コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	このコマンドをデフォルト設定に戻すには、 no dscp または default dscp フローエクスポート コンフィギュレーション コマンドを使用します。				

次に、エクスポートされたデータグラムの DSCP フィールドの値を 22 に設定する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# dscp 22
```

event manager applet

Embedded Event Manager (EEM) にアプレットを登録してアプレット コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **event manager applet** コマンドを使用します。アプレットを登録解除するには、このコマンドの **no** 形式を使用します。

event manager applet *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]
no event manager applet *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]

Syntax Description	
<i>applet-name</i>	アプレット ファイルの名前。
authorization	(任意) アプレットの AAA 許可タイプを指定します。
bypass	(任意) EEM の AAA 許可タイプのバイパスを指定します。
class	(任意) EEM ポリシー クラスを指定します。
<i>class-options</i>	(任意) EEM ポリシー クラス。次のいずれかを指定できます： <ul style="list-style-type: none"> • class-letter: 各ポリシークラスを識別する A ~ Z の文字。任意の class-letter を 1 つ指定できます。 • default: デフォルトクラスに登録されたポリシーを指定します。
trap	(任意) ポリシーがトリガーされたときに簡易ネットワーク管理プロトコル (SNMP) トラップを生成します。

Command Default EEM アプレットは登録されません。

Command Modes グローバル コンフィギュレーション (config)

Command History

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines EEM アプレットは、イベントスクリーニング基準とイベント発生時に実行するアクションを定義する簡潔な方法です。

アプレット コンフィギュレーションでは、**event** コンフィギュレーション コマンドを 1 つだけ使用できます。アプレット コンフィギュレーション サブモードが終了し、**event** コマンドが存在しない場合は、アプレットにイベントが関連付けられていないことを示す警告が表示されます。イベントが指定されていない場合、このアプレットは登録されたと判断されないため、アプレットは表示されません。このアプレットにアクションが割り当てられない場合、イベントはトリガーされますが、アクションは実行されません。1 つのアプレット コンフィギュレーション内で複数

の **action** アプレット コンフィギュレーション コマンドが使用できます。登録済みのアプレットを表示するには、**show event manager policy registered** コマンドを使用します。

アプレット コンフィギュレーション モードを終了しないと既存のアプレットが置き換えられないため、EEM アプレットを変更する前に、このコマンドの **no** 形式を使用して登録を解除します。アプレット コンフィギュレーション モードでアプレットを修正中であっても、既存のアプレットを実行できます。アプレット コンフィギュレーション モードを終了すると、古いアプレットが登録解除され、新しいバージョンが登録されます。



Note 部分的な変更は行わないでください。EEMは、すでに登録されているポリシーの部分的な変更をサポートしません。EEM ポリシーは、変更で再登録する前に、常に登録解除する必要があります。

action コンフィギュレーション コマンドは、**label** 引数を使用することで一意に識別できます。**label** 引数には任意の文字列値が使用できます。アクションは、**label** 引数をソートキーとして、英数字のキーの昇順にソートされ、この順序で実行されます。

EEMは、ポリシー自体に含まれているイベントの指定内容に基づいて、ポリシーをスケジューリングおよび実行します。アプレット コンフィギュレーション モードが終了するとき、EEMは、入力された **event** コマンドと **action** コマンドを検査し、指定されたイベントの発生時に実行されるようにアプレットを登録します。

EEM ポリシーは、登録されたときに **class class-letter** が指定されている場合はクラスに割り当てられます。クラスなしで登録された EEM ポリシーは、**default** クラスに割り当てられます。**default** をクラスとして保持するスレッドは、スレッドが作業に利用可能であるとき、デフォルトクラスにサービスを提供します。特定のクラス文字に割り当てられたスレッドは、スレッドが作業に利用可能であるとき、クラス文字が一致する任意のポリシーをサービスします。

EEM 実行スレッドが、指定されたクラスのポリシー実行に利用可能でない場合で、クラスのスケジューラールールが設定されている場合は、ポリシーは該当クラスのスレッドが実行可能になるまで待ちます。同じ入力イベントからトリガーされた同期ポリシーは、同一の実行スレッドにスケジュールされなければなりません。ポリシーは、**queue_priority** をキューイング順序として使用し、各クラスの別々のキューにキューイングされます。

ポリシーがトリガーされると、AAA が設定されている場合は、許可のために AAA サーバに接続します。**authorization bypass** キーワードの組み合わせを使用して、AAA サーバへの接続をスキップし、ポリシーをただちに実行することができます。EEM は、AAA バイパス ポリシー名をリストに保存します。このリストは、ポリシーがトリガーされたときに検査されます。一致が見つかった場合、AAA 許可はバイパスされます。

EEM ポリシーによって設定されたコマンドの許可を避けるために、EEM は AAA が提供する名前付き方式リストを使用します。これらの名前付き方式リストは、コマンド許可を持たないように設定できます。

次に、AAA の設定例を示します。

この設定は、192.168.10.1 のポート 10000 に TACACS+ サーバを想定しています。TACACS+ サーバがイネーブルでない場合、コンフィギュレーションコマンドは、コンソールで許可されます。ただし、EEM ポリシーとアプレット CLI の相互動作は失敗します。

```
enable password lab
aaa new-model
tacacs-server host 128.107.164.152 port 10000
tacacs-server key cisco
aaa authentication login consoleline none
aaa authorization exec consoleline none
aaa authorization commands 1 consoleline none
aaa authorization commands 15 consoleline none
line con 0
  exec-timeout 0 0
  login authentication consoleline
aaa authentication login default group tacacs+ enable
aaa authorization exec default group tacacs+
aaa authorization commands 1 default group tacacs+
aaa authorization commands 15 default group tacacs+
```

authorization キーワード、**class** キーワード、**trap** キーワードは任意の組み合わせで使用できます。

Examples

次に、IPSLAping1 という名前の EEM アプレットが登録され、指定された SNMP オブジェクト ID の値と完全一致する（正常な IP SLA ICMP エコー動作を表す）場合に実行される例を示します（これは **ping** コマンドに相当します）。エコー操作が失敗した場合は 4 つのアクションがトリガーされ、イベントモニタリングは 2 回目の失敗後までディセーブルにされます。サーバへの ICMP エコー動作が失敗したことを示すメッセージが syslog に送信され、SNMP トラップが生成され、EEM はアプリケーション固有のイベントをパブリッシュし、IPSLA1F というカウンタが値 1 で増分されます。

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

次に、名前 one、クラス A でアプレットを登録し、タイマーイベントディテクタが 10 秒ごとにイベントをトリガーするアプレット コンフィギュレーションモードを開始する例を示します。イベントがトリガーされると、**action syslog** コマンドにより、syslog にメッセージ「hello world」が書き込まれます。

```
Router(config)# event manager applet one class A
Router(config-applet)# event timer watchdog time 10
Router(config-applet)# action syslog syslog msg "hello world"
Router(config-applet)# exit
```

次に、名前 one、クラス A でアプレットを登録するときに、AAA 許可をバイパスする例を示します。

```
Router(config)# event manager applet one class A authorization bypass
Router(config-applet)#
```

Related Commands

コマンド	説明
show event manager policy registered	登録されている EEM ポリシーを表示します。

export-protocol netflow-v9

NetFlow バージョン 9 エクスポートを Flexible NetFlow エクスポートのエクスポートプロトコルとして設定するには、フロー エクスポート コンフィギュレーション モードで **export-protocol netflow-v9** コマンドを使用します。

export-protocol netflow-v9

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default NetFlow バージョン 9 がイネーブルです。

Command Modes フロー エクスポート コンフィギュレーション

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デバイスは NetFlow v5 エクスポートフォーマットをサポートしていません。NetFlow v9 エクスポートフォーマットのみがサポートされています。

次の例では、NetFlow バージョン 9 エクスポートを NetFlow エクスポートのエクスポートプロトコルとして設定します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# export-protocol netflow-v9
```

export-protocol netflow-v5

NetFlow バージョン 5 エクスポートを Flexible NetFlow エクスポートのエクスポートプロトコルとして設定するには、フロー エクスポート コンフィギュレーション モードで **export-protocol netflow-v5** コマンドを使用します。

export-protocol netflow-v5

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default NetFlow バージョン 5 がイネーブルです。

Command Modes フロー エクスポート コンフィギュレーション

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

exporter

フローモニタのフローエクスポートを追加するには、適切なコンフィギュレーションモードで **exporter** コマンドを使用します。フローモニタ用のフローエクスポートを削除するには、このコマンドの **no** 形式を使用します。

exporter *exporter-name*
no exporter *exporter-name*

Syntax Description	<i>exporter-name</i> 事前に設定したフローエクスポートの名前				
Command Default	エクスポートは設定されていません。				
Command Modes	フロー モニタ コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines **exporter** コマンドを使用してフローモニタにフローエクスポートを適用するには、**flow exporter** コマンドを使用して事前にフローエクスポートを作成しておく必要があります。

このコマンドをデフォルト設定に戻すには、**no exporter** または **default exporter** フロー モニタ コンフィギュレーション コマンドを使用します。

Examples

次の例では、フローモニタのエクスポートを設定します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# exporter EXPORTER-1
```

fconfigure

チャンネルのオプションを指定するには、TCL コンフィギュレーション モードで **fconfigure** コマンドを使用します。

fconfigure *channel-name* **remote** [*host port*] **broadcast** *boolean* **vrf** *vrf-table-name*

Syntax Description	<p>remote リモートセッションを設定します。IPv4 アドレスと IPv6 アドレスの両方をサポートします。</p> <p>broadcast ブロードキャストを有効または無効にします。オプションの値は適切なブール値である必要があります。</p> <p>vrf 指定されたソケットのローカル VRF テーブル名を返します。指定されたソケットに VRF テーブルが設定されていない場合、TCL_ERROR が返され、「No VRF table configured」がインタープリタの結果に追加されます。</p>				
Command Default					
Command Modes	TCL コンフィギュレーション モード				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.2.1</td> <td>myvrf キーワードが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Amsterdam 17.2.1	myvrf キーワードが導入されました。
リリース	変更内容				
Cisco IOS XE Amsterdam 17.2.1	myvrf キーワードが導入されました。				

flow exporter

Flexible NetFlow フローエクスポートを作成するか既存の Flexible NetFlow フローエクスポートを変更し、Flexible NetFlow フロー エクスポート コンフィギュレーション モードを開始するには、グローバルコンフィギュレーションモードで **flow exporter** コマンドを使用します。Flexible NetFlow フローエクスポートを削除するには、このコマンドの **no** 形式を使用します。

flow exporter *exporter-name*
no flow exporter *exporter-name*

Syntax Description

exporter-name 作成または変更するフローエクスポートの名前。

Command Default

Flexible NetFlow フローエクスポートは、コンフィギュレーション内には存在しません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローエクスポートでは、フローモニタキャッシュ内のデータをリモートシステム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。フローエクスポートは、コンフィギュレーションで別のエンティティとして作成されます。フローエクスポートは、フローモニタにデータエクスポート機能を提供するためにフローモニタに割り当てられます。複数のフローエクスポートを作成して、1つまたは複数のフローモニタに適用すると、いくつかのエクスポート先を指定することができます。1つのフローエクスポートを作成し、いくつかのフローモニタに適用することができます。

Examples

次に、FLOW-EXPORTER-1 という名前のフローエクスポートを作成し、Flexible NetFlow フロー エクスポート コンフィギュレーション モードを開始する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

flow monitor

フローモニタを作成するか、または既存のフローモニタを変更して、フローモニタコンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **flow monitor** コマンドを使用します。フローモニタを削除するには、このコマンドの **no** 形式を使用します。

flow monitor *monitor-name*
no flow monitor *monitor-name*

Syntax Description

monitor-name 作成または変更するフローモニタの名前。

Command Default

Flexible NetFlow フローモニタは、コンフィギュレーション内には存在しません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローモニタは Flexible NetFlow のネットワークトラフィックの監視を実行するコンポーネントで、インターフェイスに適用されます。フローモニタは、フローレコードとキャッシュで構成されます。フローモニタを作成した後に、フローモニタにレコードを追加します。フローモニタのキャッシュは、フローモニタが最初のインターフェイスに適用されると自動的に作成されます。フローデータは、モニタリングプロセス中にネットワークトラフィックから収集されます。このデータ収集は、フローモニタのレコード内のキーフィールドおよび非キーフィールドに基づいて実行され、フローモニタのキャッシュに保存されます。

Examples

次の例では、FLOW-MONITOR-1 という名前のフローモニタを作成し、フローモニタコンフィギュレーションモードを開始します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

flow record

Flexible NetFlow フローレコードを作成するか既存の Flexible NetFlow フローレコードを変更し、Flexible NetFlow フローレコード コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **flow record** コマンドを使用します。Flexible NetFlow レコードを削除するには、このコマンドの **no** 形式を使用します。

flow record *record-name*
no flow record *record-name*

Syntax Description

record-name 作成または変更するフローレコードの名前。

Command Default

Flexible NetFlow フローレコードは設定されていません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードでは、フロー内のパケットを識別するために Flexible NetFlow で使用するキーとともに、Flexible NetFlow がフローについて収集する他の関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フローレコードを定義できます。デバイスは、幅広いキーセットをサポートします。フローレコードでは、フロー単位で収集するカウンタのタイプも定義します。64 ビットのパケットまたはバイトカウンタを設定できます。

Examples

次に、FLOW-RECORD-1 という名前のフローレコードを作成し、Flexible NetFlow フローレコード コンフィギュレーション モードを開始する例を示します。

```
Device(config)# flow record FLOW-RECORD-1  
Device(config-flow-record)#
```

ip wccp

Web キャッシュサービスをイネーブルにし、アプリケーションエンジンで定義されたダイナミックサービスに対応するサービス番号を指定するには、デバイスで **ip wccp** グローバルコンフィギュレーション コマンドを使用します。サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip wccp {web-cache | service-number} [group-address groupaddress] [group-list access-list]
[redirect-list access-list] [password encryption-number password]
no ip wccp {web-cache | service-number} [group-address groupaddress] [group-list access-list]
[redirect-list access-list] [password encryption-number password]
```

Syntax Description

web-cache	Web キャッシュ サービスを指定します（WCCP バージョン 1 とバージョン 2）。
<i>service-number</i>	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0～254 の範囲で指定できます。サービスの最大数（ web-cache キーワードで指定する Web キャッシュサービスを含む）は 256 です。
group-address <i>groupaddress</i>	（任意）サービスグループに参加するためにデバイスおよびアプリケーションエンジンが使用するマルチキャストグループアドレスを指定します。
group-list <i>access-list</i>	（任意）マルチキャストグループアドレスが使用されない場合、サービスグループに加入しているアプリケーションエンジンに対応する有効な IP アドレスのリストを指定します。
redirect-list <i>access-list</i>	（任意）ホストから特定のホストまたは特定のパケットのリダイレクト サービスを指定します。
password <i>encryption-number</i> <i>password</i>	（任意）暗号化番号を指定します。指定できる範囲は 0～7 です。暗号化しない場合は 0、独自の場合は 7 を使用します。また、7 文字以内でパスワード名を指定します。デバイスは、パスワードと MD5 認証値を組み合わせ、デバイスとアプリケーションエンジンとの接続にセキュリティを確保します。デフォルトでは、パスワードは設定されておらず、認証も実行されていません。

Command Default

WCCP サービスがデバイスでイネーブルにされていません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

シスコエクスプレスフォワーディングスイッチングがイネーブルのとき、WCCPの透過的キャッシングはネットワーク アドレス変換 (NAT) をバイパスします。この状況に対処するには、発信方向でWCCP透過キャッシングを設定し、コンテンツエンジンインターフェイスでCisco Express Forwarding スwitchingを有効にし、**ip wccp web-cache redirect out** コマンドを指定します。キャッシュに面するルータインターフェイスで**ip wccp redirect exclude in** コマンドを指定し、内部インターフェイスの着信方向にWCCPを設定します。この設定は、そのインターフェイスに到着したパケットのリダイレクションを回避します。

サービスグループを設定するときにリダイレクトリストを含めることもできます。指定されたリダイレクトリストは、NAT (送信元) IP アドレスを含むパケットを拒否して、リダイレクションを阻止します。

このコマンドは、指定されたサービス番号またはWeb キャッシュサービス名のサポートをイネーブルまたはディセーブルにするようデバイスに指示します。サービス番号は0～254の範囲で指定できます。サービス番号または名前がイネーブルになると、ルータはサービスグループの確立に参加できます。

no ip wccp コマンドが入力されると、デバイスはサービスグループへの参加を終了し、引き続きサービスが設定されているインターフェイスがなければ領域の割り当てを解除し、他のサービスが設定されていない場合はWCCPタスクを終了します。

web-cache に続くキーワードと *service-number* 引数はオプションで、任意の順序で指定できますが、1回しか指定できません。

例

次に、Web キャッシュ、アプリケーション エンジンまたはサーバに接続されたインターフェイス、およびクライアントに接続するインターフェイスを設定する例を示します。

```
Device(config)# ip wccp web-cache
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no switchport
Device(config-if)# ip address 172.20.10.30 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)#
*Dec 6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Device(config-if)# ip address 175.20.20.10 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# ip wccp web-cache group-listen
Device(config-if)# exit
```

ip flow monitor

デバイスが受信または転送する IPv4 トラフィックの Flexible NetFlow フローモニタをイネーブルにするには、インターフェイス コンフィギュレーションモードで **ip flow monitor** コマンドを使用します。フローモニタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip flow monitor monitor-name [sampler sampler-name] {input | output}
no ip flow monitor monitor-name [sampler sampler-name] {input | output}
```

Syntax Description

monitor-name	インターフェイスに適用するフロー モニタの名前。
sampler sampler-name	(任意) フローモニタ用に指定したフローサンプラーの名前をイネーブルにします。
input	デバイスがインターフェイスで受信する IPv4 トラフィックをモニタします。
output	デバイスがインターフェイスで送信する IPv4 トラフィックをモニタします。

Command Default

フローモニタはイネーブルになっていません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ip flow monitor コマンドを使用して、任意のインターフェイスにフローモニタを適用するには、事前に **flow monitor** グローバル コンフィギュレーションコマンドを使用して、フローモニタを作成しておく必要があります。

フローモニタにサンプラーを追加すると、その名前付きサンプラーによって選択されたパケットだけがキャッシュに保存され、フローを形成します。サンプラーを使用するたびに、その使用に対応する統計情報が別個に保存されます。

インターフェイスですでにイネーブルになっているフローモニタにサンプラーを追加することはできません。まず、そのフローモニタをインターフェイスから削除してから、同じフローモニタをサンプラーとともに追加する必要があります。



Note 想定される使用状況を得るには、各フローの統計情報をスケールする必要があります。たとえば、100 パケットにつき 1 パケットをサンプリングするサンプラーを使用した場合は、パケットカウンタとバイトカウンタを 100 倍する必要があります。

次に、入力トラフィックのモニタリングのためにフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

次に、同一のインターフェイスで入出力トラフィックのモニタリングのために同じフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

次に、同一のインターフェイスで入出力トラフィックのモニタリングのために2つの異なるフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

次に、異なる2つのインターフェイスで入出力トラフィックのモニタリングのために同じフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# exit
Device(config)# interface gigabitethernet2/0/3
Device(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

次に、サンプラーによってサンプリングされる入力パケット数を制限した状態で、入力トラフィックをモニタするようにフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

次の例では、サンプラーなしでインターフェイスでイネーブルになっているフローモニタにサンプラーを追加する場合の動作を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フローモニタをサンプラーと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ipv6 flow monitor

デバイスが受信または転送する IPv6 トラフィックのフローモニタをイネーブルにするには、インターフェイス コンフィギュレーションモードで **ipv6 flow monitor** コマンドを使用します。フローモニタをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ipv6 flow monitor monitor-name [sampler sampler-name] {input|output}
no ipv6 flow monitor monitor-name [sampler sampler-name] {input|output}
```

Syntax Description

<i>monitor-name</i>	インターフェイスに適用するフロー モニタの名前。
sampler <i>sampler-name</i>	(任意) フローモニタ用に指定したフローサンプラーの名前をイネーブルにします。
input	デバイスがインターフェイスで受信する IPv6 トラフィックをモニタします。
output	デバイスがインターフェイスで送信する IPv6 トラフィックをモニタします。

Command Default

フローモニタはイネーブルになっていません。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ipv6 flow monitor コマンドを使用して、任意のインターフェイスにフローモニタを適用するには、事前に **flow monitor** グローバル コンフィギュレーション コマンドを使用して、フローモニタを作成しておく必要があります。

フローモニタにサンプラーを追加すると、その名前付きサンプラーによって選択されたパケットだけがキャッシュに保存され、フローを形成します。サンプラーを使用するたびに、その使用に対応する統計情報が別個に保存されます。

インターフェイスですでにイネーブルになっているフローモニタにサンプラーを追加することはできません。まず、そのフローモニタをインターフェイスから削除してから、同じフローモニタをサンプラーとともに追加する必要があります。



Note 想定される使用状況を得るには、各フローの統計情報をスケールする必要があります。たとえば、100 パケットにつき 1 パケットをサンプリングするサンプラーを使用した場合は、パケットカウントとバイトカウントを 100 倍する必要があります。

次に、入力トラフィックのモニタリングのためにフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

次に、同一のインターフェイスで入出力トラフィックのモニタリングのために同じフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 output
```

次に、同一のインターフェイスで入出力トラフィックのモニタリングのために2つの異なるフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-2 output
```

次に、異なる2つのインターフェイスで入出力トラフィックのモニタリングのために同じフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# exit
Device(config)# interface gigabitethernet2/0/3
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 output
```

次に、サンプラーによってサンプリングされる入力パケット数を制限した状態で、入力トラフィックをモニタするようにフローモニタをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

次の例では、サンプラーなしでインターフェイスでイネーブルになっているフローモニタにサンプラーを追加する場合の動作を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フローモニタをサンプラーと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ipv6 deny echo reply

IPv6 マルチキャストアドレスまたはエニーキャストアドレスへの ICMP IPv6 エコー応答メッセージの生成を無効にするには、**ipv6 deny-echo-reply** コマンドをグローバル コンフィギュレーション モードで使用します。ICMP IPv6 エコー応答メッセージの生成を有効にするには、コマンドの **no** 形式を使用します。

ipv6 deny-echo-reply
no ipv6 deny-echo-reply

Command Default ICMPv6 エコー応答メッセージがデバイスから送信されます。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが追加されました。

Usage Guidelines **ipv6 deny-echo-reply** コマンドは、IPv6 マルチキャストまたはエニーキャストアドレスに対してのみ機能します。IPv6 ユニキャストアドレスのエコー応答メッセージは抑制しません。

次に、ICMPv6 エコーメッセージへの応答の送信を停止するようにデバイスを設定する例を示します。

```
Device# configure terminal
Device (config) #ipv6 deny-echo-reply
Router (config) #end
```

次に、**ipv6 deny-echo-reply** 設定を削除する例を示します。

```
Device# configure terminal
Device (config) #no ipv6 deny-echo-reply
Router (config) #end
```

match datalink dot1q priority

802.1Q (dot1q) 優先順位値をフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match datalink dot1q priority** コマンドを使用します。優先順位をフローレコードのキーフィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match datalink dot1q priority
no match datalink dot1q priority

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

優先順位フィールドはキーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

match datalink dot1q priority コマンドの観測点は、コマンドで指定されたフローレコードを含むフローモニタが適用されているインターフェイスです。

次に、802.1Q 優先順位をフローレコードのキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1  
Device(config-flow-record)# match datalink dot1q priority
```

match datalink dot1q vlan

802.1Q (dot1q) VLAN 値をフローレコードのキーフィールドとして設定するには、フローレコード コンフィギュレーション モードで **match datalink dot1q vlan** コマンドを使用します。802.1Q VLAN 値をフローレコードのキーフィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

```
match datalink dot1q vlan {input | output}
no match datalink dot1q vlan {input | output}
```

Syntax Description

input デバイスが受信しているトラフィックの VLANID をキーフィールドとして設定します。

output デバイスが送信しているトラフィックの VLANID をキーフィールドとして設定します。

Command Default

802.1Q VLAN ID はキー フィールドとして設定されていません。

Command Modes

フロー レコード コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフロー モニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

match datalink dot1q vlan コマンドの **input** および **output** キーワードは、**match datalink dot1q vlan** コマンドがネットワークトラフィックに固有の 802.1q VLAN ID に基づいてフローを作成するために使用する観測点を指定します。

次に、デバイスが受信しているトラフィックの 802.1Q VLAN ID をフローレコードのキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink dot1q vlan input
```

match datalink ethertype

パケットの EtherType をフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match datalink ethertype** コマンドを使用します。パケットの EtherType をフローレコードのキーフィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match datalink ethertype
no match datalink ethertype

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

パケットの EtherType はキーフィールドとして設定されません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

match datalink ethertype コマンドを使用して、パケットの EtherType をフローレコードのキーフィールドとして設定すると、トラフィックフローは、インターフェイスに割り当てられたフローモニタのタイプに基づいて作成されます。

- **datalink flow monitor** インターフェイスコンフィギュレーションコマンドを使用して、データリンクフローモニタがインターフェイスに割り当てられると、異なるレイヤ2プロトコルに対して一意のフローが作成されます。
- **ip flow monitor** インターフェイスコンフィギュレーションコマンドを使用して、IPフローモニタがインターフェイスに割り当てられると、異なるIPv4プロトコルに対して一意のフローが作成されます。
- **ipv6 flow monitor** インターフェイスコンフィギュレーションコマンドを使用して、IPv6フローモニタがインターフェイスに割り当てられると、異なるIPv6プロトコルに対して一意のフローが作成されます。

このコマンドをデフォルト設定に戻すには、**no match datalink ethertype** または **default match datalink ethertype** フローレコードコンフィギュレーションコマンドを使用します。

次の例では、パケットの EtherType を Flexible NetFlow フローレコードのキーフィールドとして設定しています。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink ethertype
```

match datalink mac

フローレコードのキーフィールドとして MAC アドレスを使用するように設定するには、フローレコード コンフィギュレーション モードで **match datalink mac** コマンドを使用します。フローレコードのキーフィールドとして MAC アドレスを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
match datalink mac {destination address {input | output} | source address {input | output}}
no match datalink mac {destination address {input | output} | source address {input | output}}
```

Syntax Description	destination address	キーフィールドとして宛先 MAC アドレスを使用するように設定します。
	input	入力パケットの MAC アドレスを指定します。
	output	出力パケットの MAC アドレスを指定します。
	source address	キーフィールドとして送信元 MAC アドレスを使用するように設定します。

Command Default MAC アドレスは、キー フィールドとして設定されていません。

Command Modes フロー レコード コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines フローレコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

input および **output** キーワードを使用して、**match datalink mac** コマンドで使用する観測ポイントを指定し、ネットワークトラフィックの一意の MAC アドレスに基づいてフローを作成します。



Note データリンク フロー モニタがインターフェイスまたは VLAN レコードに割り当てられている場合、非 IPv6 または非 IPv4 トラフィック用のフローだけが作成されます。

このコマンドをデフォルト設定に戻すには、**no match datalink mac** または **default match datalink mac** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、フローレコードのキーフィールドとして、デバイスによって送信されるパケットの送信元 MAC アドレスを使用するように設定します。

```
Device(config)# flow record FLOW-RECORD-1  
Device(config-flow-record)# match datalink mac source address output
```

次の例では、フローレコードのキーフィールドとして、デバイスによって受信されるパケットの宛先 MAC アドレスを使用するように設定します。

```
Device(config)# flow record FLOW-RECORD-1  
Device(config-flow-record)# match datalink mac destination address input
```

match datalink vlan

VLANIDをフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match datalink vlan** コマンドを使用します。VLAN ID をフローレコードのキーフィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

```
match datalink vlan {input|output}
no match datalink vlan {input|output}
```

Syntax Description

input デバイスが受信しているトラフィックのVLANIDをキーフィールドとして設定します。

output デバイスが送信しているトラフィックのVLANIDをキーフィールドとして設定します。

Command Default

VLAN ID はキー フィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

match datalink vlan コマンドの **input** および **output** キーワードは、**match datalink vlan** コマンドがネットワークトラフィックに固有のVLANIDに基づいてフローを作成するために使用する観測点を指定します。

次に、デバイスが受信しているトラフィックのVLAN ID をフローレコードのキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink vlan input
```

match flow cts

フローレコードの CTS 送信元グループタグおよび宛先グループタグを設定するには、フローレコードコンフィギュレーションモードで **match flow cts** コマンドを使用します。グループタグをフローレコードのキーフィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

```
match flow cts {source | destination} group-tag
no match flow cts {source | destination} group-tag
```

Syntax Description

cts destination group-tag	CTS 宛先フィールドグループをキーフィールドとして設定します。
cts source group-tag	CTS 送信元フィールドグループをキーフィールドとして設定します。

Command Default

CTS 宛先または送信元フィールドグループ、フロー方向およびフロー サンプラー ID は、キーフィールドとして設定されていません。

Command Modes

Flexible NetFlow フローレコードコンフィギュレーション (config-flow-record)
ポリシー インライン コンフィギュレーション (config-if-policy-inline)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、送信元グループタグをキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow cts source group-tag
```

match flow direction

フロー方向をフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match flow direction** コマンドを使用します。フロー方向をフローレコードのキーフィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match flow direction
no match flow direction

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

フロー方向はキーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

match flow direction コマンドは、フローの方向をキーフィールドとしてキャプチャします。この機能は、入力フローと出力フローに対して単一のフローモニタが設定されている場合に最も役立ちます。また、入力と出力で1回ずつ、2回モニタされているフローを見つけ、除外するために使用することができます。このコマンドは、2つのフローが反対方向に流れている場合に、エクスポートされたデータ内のフローのペアを一致させるために役立つ場合もあります。

次に、フローがモニタされた方向をキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow direction
```

match interface

入力インターフェイスと出力インターフェイスをフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match interface** コマンドを使用します。入力インターフェイスと出力インターフェイスをフローレコードのキーフィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

```
match interface {input | output}
no match interface {input | output}
```

Syntax Description

input 入力インターフェイスをキーフィールドとして設定します。

output 出力インターフェイスをキーフィールドとして設定します。

Command Default

入力インターフェイスと出力インターフェイスは、キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、入力インターフェイスをキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface input
```

次に、出力インターフェイスをキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface output
```

match ipv4

フローレコードのキーフィールドとして1つ以上のIPv4フィールドを設定するには、フローレコードコンフィギュレーションモードで **match ipv4** コマンドを使用します。フローレコードのキーフィールドとして1つ以上のIPv4フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
match ipv4 {destination address | protocol | source address | tos | ttl | version}
no match ipv4 {destination address | protocol | source address | tos | ttl | version}
```

Syntax Description

destination address	キーフィールドとしてIPv4宛先アドレスを設定します。詳細については、 <i>match ipv4 destination address</i> を参照してください。
protocol	キーフィールドとしてIPv4プロトコルを設定します。
source address	キーフィールドとしてIPv4宛先アドレスを設定します。詳細については、 <i>match ipv4 source address</i> を参照してください。
tos	キーフィールドとしてIPv4 ToS を設定します。
ttl	フローレコードのキーフィールドとしてIPv4 存続可能時間 (TTL) フィールドを設定します。詳細については、 <i>match ipv4 ttl</i> を参照してください。
version	キーフィールドとしてIPv4 ヘッダーの IP バージョンを設定します。

Command Default

ユーザ定義のフローレコードのキーフィールドとして1つ以上のIPv4フィールドを使用する設定は、イネーブルになっていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次の例では、キーフィールドとしてIPv4プロトコルを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 protocol
```

match ipv4 destination address

IPv4 宛先アドレスをフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match ipv4 destination address** コマンドを使用します。IPv4 宛先アドレスをフローレコードのキーフィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 destination address
no match ipv4 destination address

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IPv4 宛先アドレスはキーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 destination address** または **default match ipv4 destination address** フローレコードコンフィギュレーションコマンドを使用します。

次の例では、IPv4 宛先アドレスをフローレコードのキーフィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 destination address
```

match ipv4 source address

IPv4 送信元アドレスをフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match ipv4 source address** コマンドを使用します。フローレコードのキーフィールドとしてIPv4送信元アドレスを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 source address
no match ipv4 source address

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IPv4 送信元アドレスがキーフィールドとして設定されません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 source address** または **default match ipv4 source address** フローレコードコンフィギュレーションコマンドを使用します。

次に、キーフィールドとしてIPv4送信元アドレスを設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 source address
```

match ipv4 ttl

フローレコードのキーフィールドとしてIPv4 存続可能時間（TTL）フィールドを設定するには、フローレコードコンフィギュレーションモードで **match ipv4 ttl** コマンドを使用します。フローレコードのキーフィールドとしてIPv4 TTL を使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 ttl
no match ipv4 ttl

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IPv4 存続可能時間（TTL）フィールドは、キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match ipv4 ttl** コマンドを使用して定義されます。

次に、キーフィールドとして IPv4 TTL を設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 ttl
```

match ipv6

フローレコードのキーフィールドとして1つ以上のIPv6フィールドを設定するには、フローレコードコンフィギュレーションモードで **match ipv6** コマンドを使用します。フローレコードのキーフィールドとして1つ以上のIPv6フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
match ipv6 {destination address | hop-limit | protocol | source address | traffic-class | version}
no match ipv6 {destination address | hop-limit | protocol | source address | traffic-class | version}
```

Syntax Description	destination address	hop-limit	protocol	source address	traffic-class	version
	キーフィールドとしてIPv4宛先アドレスを設定します。詳細については、 <i>match ipv6 destination address</i> を参照してください。	キーフィールドとしてIPv6ホップリミットを設定します。詳細については、 <i>match ipv6 hop limit</i> を参照してください。	キーフィールドとしてIPv6プロトコルを設定します。	キーフィールドとしてIPv4宛先アドレスを設定します。詳細については、 <i>match ipv6 source address</i> を参照してください。	キーフィールドとしてIPv6トラフィッククラスを設定します。	キーフィールドとしてIPv6ヘッダーのIPv6バージョンを設定します。

Command Default IPv6の各フィールドは、キーフィールドとして設定されていません。

Command Modes フローレコードコンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次の例では、キーフィールドとしてIPv6プロトコルフィールドを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 protocol
```

match ipv6 destination address

IPv6 宛先アドレスをフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match ipv6 destination address** コマンドを使用します。IPv6 宛先アドレスをフローレコードのキーフィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 destination address
no match ipv6 destination address

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IPv6 宛先アドレスはキーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 destination address** または **default match ipv6 destination address** フローレコードコンフィギュレーションコマンドを使用します。

次の例では、キーフィールドとして IPv6 宛先アドレスを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 destination address
```

match ipv6 hop-limit

フローレコードのキーフィールドとしてIPv6 ホップリミットを設定するには、フローレコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。フローレコードのキーフィールドとしてIPv6パケットのセクションを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 hop-limit
no match ipv6 hop-limit

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

ユーザ定義のフローレコードのキーフィールドとしてIPv6 ホップリミットを使用する設定は、デフォルトでイネーブルになっていません。

Command Modes

フローレコード コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、キーフィールドとしてフローパケットのホップリミットを設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 hop-limit
```

match ipv6 source address

IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 source address** コマンドを使用します。フロー レコードのキーフィールドとしてIPv6送信元アドレスを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 source address
no match ipv6 source address

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IPv6 送信元アドレスはキー フィールドとして設定されていません。

Command Modes

フロー レコード コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フロー レコードをフロー モニタで使用するには、1つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 source address** または **default match ipv6 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、IPv6 送信元アドレスをキー フィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 source address
```

map platform-type

パラメータマップ属性フィルタ基準をプラットフォームタイプに設定するには、パラメータマップフィルタモードで **map platform-type** コマンドを使用します。この基準を削除するには、このコマンドの **no** 形式を使用します。

```
map-number map platform-type { {eq | not-eq | regex} platform-type }
no map-number map platform-type { {eq | not-eq | regex} platform-type }
```

Syntax Description

map-number	パラメータマップ番号。
eq	フィルタタイプ名がプラットフォームタイプ名と同じであることを指定します。
not-eq	フィルタタイプ名がプラットフォームタイプ名と同じでないことを指定します。
regex	フィルタタイプ名が正規表現であることを指定します。
platform-type	パラメータマップ属性フィルタ基準のプラットフォームタイプ。

Command Default

デフォルトの動作や値はありません。

Command Modes

パラメータマップフィルタ (config-parameter-map-filter)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

Examples

次に、パラメータマップ属性フィルタ基準をプラットフォームタイプに設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para
Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx
```

Related Commands

コマンド	説明
parameter-map type subscriber attribute-to-service	サブスクリイバパラメータマップを設定し、パラメータマップフィルタコンフィギュレーションモードを開始します。

match transport

フローレコードのキーフィールドとして1つ以上のトランスポートフィールドを設定するには、フローレコードコンフィギュレーションモードで **match transport** コマンドを使用します。フローレコードのキーフィールドとして1つ以上のトランスポートフィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
match transport {destination-port | icmp ipv4 | icmp ipv6 | igmp type | source-port}
no match transport {destination-port | icmp ipv4 | icmp ipv6 | igmp type | source-port}
```

Syntax Description

destination-port	キーフィールドとしてトランスポート宛先ポートを設定します。
icmp ipv4	ICMP IPv4 のタイプフィールドとコードフィールドをキーフィールドとして設定します。詳細については、 match transport icmp ipv4, on page 1024 を参照してください。
icmp ipv6	ICMP IPv6 のタイプフィールドとコードフィールドをキーフィールドとして設定します。詳細については、 match transport icmp ipv6, on page 1025 を参照してください。
igmp type	システム稼働時間に基づくタイムスタンプをキーフィールドとして設定します。
source-port	キーフィールドとしてトランスポート送信元ポートを設定します。

Command Default

トランスポートフィールドは、キーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次の例では、宛先ポートをキーフィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport destination-port
```

次の例では、送信元ポートをキーフィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport source-port
```

match transport icmp ipv4

ICMP IPv4 のタイプフィールドとコードフィールドをフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match transport icmp ipv4** コマンドを使用します。ICMP IPv4 のタイプフィールドとコードフィールドをフローレコードのキーフィールドとして使用するのをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
match transport icmp ipv4 {code | type}
no match transport icmp ipv4 {code | type}
```

Syntax Description

code ICMP IPv4 コードをキーフィールドとして設定します。

type ICMP IPv4 タイプをキーフィールドとして設定します。

Command Default

ICMP IPv4 のタイプフィールドとコードフィールドはキーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、ICMP IPv4 コードフィールドをキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 code
```

次に、ICMP IPv4 タイプフィールドをキーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv6

ICMP IPv6 のタイプフィールドとコードフィールドをフローレコードのキーフィールドとして設定するには、フローレコードコンフィギュレーションモードで **match transport icmp ipv6** コマンドを使用します。ICMP IPv6 のタイプフィールドとコードフィールドをフローレコードのキーフィールドとして使用するのをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
match transport icmp ipv6 {code | type}
no match transport icmp ipv6 {code | type}
```

Syntax Description

code IPv6 ICMP コードをキーフィールドとして設定します。

type IPv6 ICMP タイプをキーフィールドとして設定します。

Command Default

ICMP IPv6 タイプフィールドおよびコードフィールドはキーフィールドとして設定されていません。

Command Modes

フローレコードコンフィギュレーション

Command History

リリース	変更内容
------	------

Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
--------------------------	-----------------

Usage Guidelines

フローレコードをフローモニタで使用するには、1つ以上のキーフィールドが必要になります。キーフィールドはフローを区別するものです。各フローのキーフィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次の例では、IPv6 ICMP コードフィールドをキーフィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 code
```

次の例では、IPv6 ICMP タイプフィールドをキーフィールドとして設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 type
```

match platform-type

プラットフォームタイプに基づいて制御クラスを評価するには、コントロールクラスマップフィルタ モードで **match platform-type** コマンドを使用します。この条件を削除するには、このコマンドの **no** 形式を使用します。

match platform-type *platform-name*
no match platform-type *platform-name*

Syntax Description

platform-name プラットフォームの名前。

Command Default

デフォルトの動作や値はありません。

Command Modes

コントロール クラスマップ フィルタ (config-filter-control-classmap)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

Examples

次に、クラスマップフィルタでプラットフォームタイプを照合するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match platform-type C9xxx
```

Related Commands

コマンド	説明
class-map type control subscriber	制御クラスを作成し、制御クラスマップ フィルタ モードを開始します。

mode random 1 out-of

ランダムサンプリングを有効にし、Flexible NetFlow サンプラーのパケット間隔を指定するには、サンプラー コンフィギュレーションモードで **mode random 1 out-of** コマンドを使用します。Flexible NetFlow サンプラーのパケット間隔情報を削除するには、このコマンドの **no** 形式を使用します。

mode random 1 out-of *window-size*
no mode

Syntax Description

window-size パケットを選択するウィンドウ サイズを指定します。指定できる範囲は 2 ～ 1024 です。

Command Default

サンプラーのモードとパケット間隔は設定されていません。

Command Modes

サンプラー コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デバイスでは、計 4 つの固有のサンプラーがサポートされています。パケットは、トラフィック パターンのバイアスを除外し、モニタリングを回避するためのユーザによる試行を無効にする方法で選択されます。



Note **deterministic** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

Examples

次の例では、ウィンドウ サイズ 1000 でランダム サンプリングをイネーブルにします。

```
Device(config)# sampler SAMPLER-1  
Device(config-sampler)# mode random 1 out-of 1000
```

monitor capture (interface/control plane)

接続ポイントおよびパケットフロー方向を指定してモニタキャプチャポイントを設定する、またはキャプチャポイントに接続ポイントを追加するには、特権 EXEC モードで **monitor capture** コマンドを使用します。指定した接続ポイントおよびパケットフロー方向でモニタキャプチャを無効にする、またはキャプチャポイント上の複数の接続ポイントのいずれかを無効にするには、このコマンドの **no** 形式を使用します。

```
monitor capture {capture-name} {interface interface-type interface-id | control-plane} {in | out | both}
no monitor capture {capture-name} {interface interface-type interface-id | control-plane} {in | out | both}
```

Syntax Description

<i>capture-name</i>	定義するキャプチャの名前。
interface <i>interface-type interface-id</i>	<i>interface-type</i> および <i>interface-id</i> とのインターフェイスを接続ポイントとして指定します。引数の意味は次のとおりです。 <ul style="list-style-type: none"> • GigabitEthernet <i>interface-id</i>: ギガビットイーサネット IEEE 802.3z インターフェイス。 • vlan <i>vlan-id</i>: VLAN。 <i>vlan-id</i> の範囲は 1 ~ 4095 です。
control-plane	コントロールプレーンを接続ポイントとして指定します。
in out both	キャプチャするトラフィックの方向を指定します。

Command Default

Wireshark キャプチャは設定されていません。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

接続ポイントがこのコマンドを使用してキャプチャポイントに関連付けられると、方向を変更する唯一の方法は、このコマンドの **no** 形式を使用して接続ポイントを削除し、新しい方向に接続ポイントを再接続することです。接続ポイントの方向は上書きできません。

接続ポイントがキャプチャポイントから削除され、1つの接続ポイントのみが関連付けられている場合、キャプチャポイントは効率的に削除されます。

このコマンドを別の接続ポイントで再実行することで、複数の接続ポイントをキャプチャポイントと関連付けることができます。次に例を示します。

インターフェイスの出力方向にキャプチャされたパケットは、スイッチの書き換えによって行われた変更（TTL、VLAN タグ CoS、チェックサム、および MAC アドレス、DSCP、プレシデント、UP など）が反映されないこともあります。

特定の順序はキャプチャ ポイントを定義する場合には適用されません。任意の順序でキャプチャ ポイントパラメータを定義できます。Wireshark CLI では、単一行のパラメータ数に制限はありません。これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。

VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。

Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。

VLAN が Wireshark の接続ポイントとして使用されている場合、パケットは、入力方向でのみキャプチャされます。

例

物理インターフェイスを接続ポイントとして使用してキャプチャ ポイントを定義するには次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```



Note 2 つ目のコマンドは、キャプチャ ポイントのコア フィルタを定義します。これは、キャプチャポイントが機能するために必要です。

複数の接続ポイントを持つキャプチャ ポイントを定義するには次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap control-plane in
Device# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/1 in
      monitor capture mycap control-plane in
```

複数の接続ポイントで定義されたキャプチャ ポイントから接続ポイントを削除するには次を実行します。

```
Device# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/1 in
      monitor capture mycap control-plane in
Device# no monitor capture mycap control-plane
Device# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/1 in
```

monitor capture buffer

モニタキャプチャ（WireShark）のバッファを設定するには、特権 EXEC モードで **monitor capture buffer** コマンドを使用します。モニタキャプチャバッファを無効にする、またはバッファを循環バッファからデフォルトの線形バッファに戻すには、このコマンドの **no** 形式を使用します。

```
monitor capture {capture-name} buffer {circular [size buffer-size ] | size buffer-size}
no monitor capture {capture-name} buffer [circular ]
```

Syntax Description

capture-name バッファが設定されるキャプチャの名前。

circular バッファが循環タイプであることを指定します。循環タイプのバッファは、バッファが消費された後も以前にキャプチャされたデータを上書きすることでデータのキャプチャを継続します。

size *buffer-size* （任意）バッファのサイズを指定します。範囲は 1 ～ 100 MB です。

Command Default

線形バッファが設定されます。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

最初に WireShark のキャプチャを設定すると、小規模の循環バッファが提案されます。

例

1 MB のサイズの循環バッファを設定する場合は次を実行します。

```
Device# monitor capture mycap buffer circular size 1
```

monitor capture export

ファイルにモニタキャプチャ（WireShark）をエクスポートするには、特権 EXEC モードで **monitor capture export** コマンドを使用します。

```
monitor capture {capture-name} export file-location : file-name
```

Syntax Description

capture-name エクスポートするキャプチャの名前。

file-location : file-name （任意）キャプチャストレージファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。

- flash: オンボードフラッシュストレージ
- : USB ドライブ

Command Default

キャプチャされたパケットは保存されません。

Command Modes

特権 EXEC

Command History

リリース

変更内容

このコマンドが導入されました。

Usage Guidelines

ストレージの宛先がキャプチャバッファである場合にのみ **monitor capture export** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。キャプチャ中またはパケットキャプチャ停止後にこのコマンドを使用します。パケットキャプチャは、1 つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireShark がスタック内のスイッチで使用される場合、パケットキャプチャは前述の *file-location* で指定されたアクティブスイッチに接続されるデバイス上のみ保存されます。例: **flash1** はアクティブなスイッチに接続されています。**flash2** はセカンダリスイッチに接続されています。この場合、パケットキャプチャの保存に使用できるのは **flash1** だけです。



Note サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケットキャプチャを保存しようとするとエラーが発生する可能性があります。

例

キャプチャバッファの内容を flash ドライブの **mycap.pcap** にエクスポートするには次を実行します。

monitor capture limit

キャプチャ制限を設定するには、特権 EXEC モードで **monitor capture limit** コマンドを使用します。キャプチャ制限を削除するには、このコマンドの **no** 形式を使用します。

```
monitor capture {capture-name} limit {[duration seconds] [packet-length size] [packets num]}
no monitor capture {capture-name} limit [duration] [packet-length] [packets]
```

Syntax Description

<i>capture-name</i>	キャプチャ制限を割り当てられるキャプチャの名前。
duration <i>seconds</i>	(任意) キャプチャ期間 (秒) を指定します。範囲は 1 ~ 1000000 です。
packet-length <i>size</i>	(任意) パケット長 (バイト) を指定します。実際のパケットが特定の長さより長い場合、数がバイト引数によって示される最初のセットのバイトのみが保存されます。
packets <i>num</i>	(任意) キャプチャに対して処理されるパケット数を指定します。

Command Default

キャプチャ制限は設定されません。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

60 秒のセッション制限および 400 バイトのパケット セグメント長を設定するには次を実行します。

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture start

トラフィックトレースポイントでパケットデータのバッファへのキャプチャを開始するには、特権 EXEC モードで **monitor capture start** コマンドを使用します。

monitor capture {*capture-name*} **start**

Syntax Description

capture-name 開始するキャプチャの名前。

Command Default

バッファのコンテンツはクリアされません。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

キャプチャポイントが定義された後にパケットデータキャプチャを有効にするには、**monitor capture clear** コマンドを使用します。パケットデータのキャプチャを停止するには、**monitor capture stop** コマンドを使用します。

CPUおよびメモリなどのシステムリソースがキャプチャの開始前に使用可能であることを確認します。

例

バッファ コンテンツのキャプチャを開始するには次を実行します。

```
Device# monitor capture mycap start
```

monitor capture stop

トラフィック トレース ポイントでパケットデータのキャプチャを停止するには、特権 EXEC モードで **monitor capture stop** コマンドを使用します。

monitor capture {*capture-name*} **stop**

Syntax Description	<i>capture-name</i> 停止するキャプチャの名前。
---------------------------	-----------------------------------

Command Default	パケット データ キャプチャが進行中です。
------------------------	-----------------------

Command Modes	特権 EXEC
----------------------	---------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **monitor capture stop** コマンドを使用して、**monitor capture start** コマンドによって開始したパケットデータのキャプチャを停止します。線形および循環の2つのタイプのキャプチャ バッファを設定できます。線形バッファがいっぱいになった場合、データ キャプチャは自動的に停止します。循環バッファがいっぱいになると、データ キャプチャは最初から開始し、データは上書きされます。

例

バッファ コンテンツのキャプチャを停止するには次を実行します。

```
Device# monitor capture mycap stop
```

monitor session destination

新規にスイッチドポートアナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）宛先セッションを開始し、ネットワークセキュリティデバイス（Cisco IDS Sensor アプライアンスなど）の宛先ポート上の入力トラフィックをイネーブルにし、既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session destination** グローバルコンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから宛先インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
no monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
```

Syntax Description

session-number

interface *interface-id*

SPAN または RSPAN セッションの宛先となる有効なインターフェイスは物理ポート（ポート番号を含む）です。送信元インターフェイスタイプであり、指定できる範囲は

,

（任意）複数のインターフェイスまたは VLAN の範囲を指定します。

-

（任意）インターフェイスまたは VLAN を削除します。

encapsulation replicate

（任意）宛先インターフェイスが送信元インターフェイスと送信元インターフェイスの送信元とを指定します。選択しない場合のデフォルトは replicate の送信です。

次のキーワードは、ローカル SPAN に RSPAN を指定するときに、VLAN ID を上書きするため、パケットの送信先は、**no** 形式では無視されません。

encapsulation dot1q

（任意）宛先インターフェイスが IEEE 802.1Q 送信パケットを受け入れるように指定します。

次のキーワードは、ローカル SPAN に RSPAN を指定するときに、VLAN ID を上書きするため、パケットの送信先は、**no** 形式では無視されません。

ingress

入力トラフィック転送をイネーブルにします。

dot1q

（任意）指定された VLAN をデフォルトの送信先として着信パケットを受け入れます。

untagged	(任意) 指定された VLAN をデフォルトパケットを受け入れます。
isl	ISL カプセル化を使用して入力トラフィックを受け入れます。
remote	RSPAN 送信元または宛先セッションの RSPAN VLAN は VLAN 1 (デフォルトのクランリングおよび FDDI VLAN に予約済み) です。 RSPAN VLAN は VLAN 1 (デフォルトのクランリングおよび FDDI VLAN に予約済み) です。
vlan <i>vlan-id</i>	ingress キーワードとのみ使用された場合を設定します。

Command Default

モニタ セッションは設定されていません。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートではディセーブルになっています。

all、**local**、**range *session-range***、**remote** を **no monitor session** コマンドに指定することで、すべての SPAN および RSPAN、すべてのローカル SPAN、範囲、すべての RSPAN セッションをクリアできます。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

SPAN または RSPAN の宛先は物理ポートである必要があります。

スイッチ上またはスイッチ スタック上で、最大 64 の宛先ポートを保有できます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN (VSPAN) を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1つのポート、1つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,|-] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連のVLANまたはインターフェイスを指定するときは、カンマ(,)の前後にスペースが必要です。VLANまたはインターフェイスの範囲を指定するときは、ハイフン(-)の前後にスペースが必要です。

EtherChannel ポートを SPAN または RSPAN 宛先ポートとして設定できます。EtherChannel グループのメンバである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1X 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1X 認証はディセーブルです。IEEE 802.1X 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができます。

入力トラフィック転送がネットワークセキュリティデバイスでイネーブルの場合、宛先ポートはレイヤ2でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- **monitor session session_number destination interface interface-id** を他のキーワードなしで入力すると、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session session_number destination interface interface-id ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって決まります。
- **monitor session session_number destination interface interface-id encapsulation replicate** を他のキーワードなしで入力すると、出力のカプセル化はソースインターフェイスのカプセル化を複製し、入力転送はイネーブルになりません（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session session_number destination interface interface-id encapsulation replicate ingress** を入力した場合は、出力カプセル化は送信元インターフェイスカプセル化を複製し、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって決まります（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
```

```
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

次の例では、ある送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

次の例では、モニタリングされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
Device(config)# monitor session 10 source remote vlan 900
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
dot1q ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティデバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィックおよび入力トラフィックはタグなしです。

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
vlan 5
```

monitor session filter

フローベース SPAN（FSPAN）セッションやフローベース RSPAN（FRSPAN）送信元または宛先セッションを新しく開始する、または特定の VLAN に対して SPAN 送信元トラフィックを制限（フィルタ処理）するには、**monitor session filter** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションからフィルタを削除するには、このコマンドの **no** 形式を使用します。

```
monitor session session-number filter {vlan vlan-id [, | -] }
no monitor session session-number filter {vlan vlan-id [, | -] }
```

Syntax Description

session-number

vlan *vlan-id*

SPAN 送信元トラフィックを特定の VLAN に制限する上のフィルタとして VLAN のリストを指定します。4094 です。

,

任意) 複数の VLAN を指定します。または VLAN のカンマの前後にスペースを入れます。

-

(任意) VLAN の範囲を指定します。ハイフンの前

Command Default

モニタセッションは設定されていません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

1 つの VLAN、または複数のポートや VLAN、特定範囲のポートや VLAN でトラフィックをモニタできます。複数または一定範囲の VLAN を指定するには、[,|-] オプションを使用します。

複数の VLAN を指定するときは、カンマ (,) の前後にスペースが必要です。VLAN の範囲を指定するときは、ハイフン (-) の前後にスペースが必要です。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワークトラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタリングされます。**monitor session session_number filter vlan vlan-id** コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLAN のフィルタリングはイネーブルにできません。VLAN のフィルタリングが設定されている場合、VLAN は送信元になることができません。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、既存のセッションの SPAN トラフィックを指定の VLAN だけに制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次に、ローカル SPAN セッション 1 を作成してスタック メンバ 1 の送信元ポート 1 とスタック メンバ 2 の宛先ポートの送受信両方のトラフィックをモニタし、FSPAN セッションでアクセス リスト番号 122 を使用して IPv4 トラフィックをフィルタする例を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both  
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2  
Device(config)# monitor session 1 filter ip access-group 122
```

monitor session source

スイッチドポートアナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）送信元セッションを開始する、または既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session source** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
monitor session session_number source {interface interface-id [, | -] [both | rx | tx] | [remote] vlan vlan-id [, | -] [both | rx | tx]}
```

```
no monitor session session_number source {interface interface-id [, | -] [both | rx | tx] | [remote] vlan vlan-id [, | -] [both | rx | tx]}
```

Syntax Description

session_number

interface *interface-id*

SPAN または RSPAN セッションの送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタックメンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャンネルも有効なインターフェイスタイプであり、指定できる範囲は 1 ～ 48 です。

,

（任意）複数のインターフェイスまたは VLAN を指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。

-

（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。

both | **rx** | **tx**

（任意）モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。

remote

（任意）RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。

RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。

vlan *vlan-id*

ingress キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。

Command Default

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

物理ポート、ポート チャネル、VLAN が送信元になることができます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN (VSPAN) を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1つのポート、1つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,|-] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ (,) の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン (-) の前後にスペースが必要です。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、複数の送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

option

Flexible NetFlow のフローエクスポートのオプションのデータパラメータを設定するには、フローエクスポート コンフィギュレーションモードで **option** コマンドを使用します。フローエクスポートのオプションのデータパラメータを削除するには、このコマンドの **no** 形式を使用します。

option {**exporter-stats** | **interface-table** | **sampler-table**} [**timeout** *seconds*]

no option {**exporter-stats** | **interface-table** | **sampler-table**}

Syntax Description

exporter-stats	フローエクスポートの統計情報オプションを設定します。
interface-table	フローエクスポートのインターフェイステーブルオプションを設定します。
sampler-table	フローエクスポートのエクスポートサンプラーテーブルオプションを設定します。
timeout <i>seconds</i>	(任意) フローエクスポートのオプションの再送時間を秒単位で設定します。指定できる範囲は 1 ~ 86400 です。デフォルトは 600 です。

Command Default

タイムアウトは 600 秒です。他のすべてのオプションデータパラメータは設定されていません。

Command Modes

フローエクスポート コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

option exporter-stats コマンドを実行すると、レコード数、バイト数、送信されたパケット数など、エクスポートの統計情報が定期的に送信されます。このコマンドを使用して、コレクタは受信するエクスポートレコードのパケット損失を見積もります。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option interface-table コマンドを実行すると、オプションテーブルが定期的に送信されます。このオプションテーブルを使用して、コレクタはフローレコードに記録されている SNMP インターフェイスインデックスを各インターフェイス名にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option sampler-table コマンドを実行すると、オプションテーブルが定期的に送信されます。このオプションテーブルには、各サンプラーの設定の詳細が含まれており、これを使用して、コレクタは任意のフローレコードに記録されているサンプラー ID を、フローの統計情報のスケールアップに使用可能な設定にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

このコマンドをデフォルト設定に戻すには、**no option** または **default option** フロー エクスポート コンフィギュレーション コマンドを使用します。

次の例では、サンプラー オプション テーブルの定期的な送信をイネーブルにして、コレクタでサンプラー ID をサンプラーのタイプとレートにマッピングする方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

次の例では、レコード数、バイト数、送信されたパケット数など、エクスポートの統計情報の定期的な送信をイネーブルする方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

次の例では、オプションテーブルの定期的な送信をイネーブルにし、そのオプションテーブルをコレクタで使用して、フローレコードに記録されている SNMP インターフェイス インデックスをインターフェイス名にマッピングする方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

record

Flexible NetFlow フローモニタのフローレコードを追加するには、フローモニタ コンフィギュレーション モードで **record** コマンドを使用します。Flexible NetFlow フローモニタのフローレコードを削除するには、このコマンドの **no** 形式を使用します。

record *record-name*
no record

Syntax Description *record-name* 事前に設定したユーザ定義のフローレコードの名前。

Command Default フローレコードは設定されていません。

Command Modes フローモニタ コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines フローモニタごとに、キャッシュエントリの内容およびレイアウトを定義するレコードが必要です。フローモニタがさまざまな事前定義済みレコードフォーマットの1つを使用することも、上級ユーザが独自のレコードフォーマットを作成することもできます。



Note フローモニタで **record** コマンドのパラメータを変更する前に、**no ip flow monitor** コマンドを使用して、すべてのインターフェイスから適用済みのフローモニタを削除する必要があります。

Examples

次の例では、FLOW-RECORD-1 を使用するようにフローモニタを設定します。

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
```

sampler

Flexible NetFlow フローサンプラーを作成するか既存の Flexible NetFlow フローサンプラーを変更し、Flexible NetFlow フロー サンプラー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **sampler** コマンドを使用します。サンプラーを削除するには、このコマンドの **no** 形式を使用します。

sampler *sampler-name*
no sampler *sampler-name*

Syntax Description

sampler-name 作成または変更するフローサンプラーの名前。

Command Default

Flexible NetFlow フローサンプラーは設定されません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フローサンプラーは分析されるパケット数を制限することで、トラフィックをモニタするために Flexible NetFlow によってネットワークデバイスで生じる負荷を軽減するために使用されます。2 ~ 1024 パケットの範囲から 1 パケットの割合でサンプリング レートを設定します。フローサンプラーは、サンプリングされた Flexible NetFlow を実装するためにフローモニタとともにインターフェイスに適用されます。

フローサンプリングをイネーブルにするには、トラフィック分析に使用して、フローモニタに割り当てるレコードを設定します。インターフェイスにサンプラーを含むフローモニタを適用すると、サンプリングされたパケットはサンプラーによって指定されたレートで分析され、フローモニタに対応するフローレコードと比較されます。分析されるパケットがフローレコードによって指定された条件を満たす場合、フローモニタ キャッシュに追加されます。

Examples

次に、フロー サンプラーの名前 SAMPLER-1 を作成する例を示します。

```
Device(config)# sampler SAMPLER-1  
Device(config-sampler)#
```

show class-map type control subscriber

設定されている制御ポリシーのクラスマップ統計情報を表示するには、特権 EXEC モードで **show class-map type control subscriber** コマンドを使用します。

show class-map type control subscriber {all | name *control-class-name*}

Syntax Description	all	すべての制御ポリシーのクラスマップ統計情報を表示します。
	name <i>control-class-name</i>	指定した制御ポリシーのクラスマップ統計情報を表示します。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Examples

次に、**show class-map type control subscriber name control-class-name** コマンドの出力例を示します。

```
Device# show class-map type control subscriber name platform

Class-map          Action          Exec  Hit  Miss  Comp
-----          -
match-all platform  match platform-type C9xxx  0    0    0    0
Key:
  "Exec" - The number of times this line was executed
  "Hit" - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
           condition without a need to continue on to the end
```

show ip sla statistics

Cisco IOS IP サービスレベル契約（SLA）のすべての動作または指定された動作の現在または集約された動作ステータスおよび統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip sla statistics** コマンドを使用します。

show ip sla statistics [*operation-number* [**details**] | **aggregated** [*operation-number* | **details**] | **details**]

Syntax Description

operation-number	（任意）動作ステータスおよび統計情報を表示する動作の番号。受け入れられる値の範囲は 1 ～ 2147483647 です。
details	（任意）詳細出力を指定します。
aggregated	（任意）IP SLA 集約統計を指定します。

Command Default

稼働しているすべての IP SLA 動作の出力を表示します。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

動作の残りの継続時間、動作がアクティブかどうか、完了時刻など、IP SLA 動作の現在の状態を表示するには、**show ip sla statistics** を使用します。出力には、最後の（最近完了した）動作に対して返されたモニタリング データも含まれます。この生成された操作 ID は、基本マルチキャスト操作に対して、また操作全体の要約統計の一部として **show ip sla** コンフィギュレーション コマンドを使用すると表示されます。

あるレスポンドに対して詳細を表示するには、その特定の操作 ID に **show** コマンドを入力します。

例

次に、**show ip sla statistics** コマンドの出力例を示します。

```
Device# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
```

```
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200 OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show monitor

すべてのスイッチドポートアナライザ（SPAN）およびリモート SPAN（RSPAN）セッションに関する情報を表示するには、EXEC モードで **show monitor** コマンドを使用します。

show monitor [**session** {*session_number* | **all** | **local** | **range list** | **remote**} [**detail**]]

Syntax Description

session	（任意）指定された SPAN セッションの情報を表示します。
<i>session_number</i>	
all	（任意）すべての SPAN セッションを表示します。
local	（任意）ローカル SPAN セッションだけを表示します。
range list	（任意）一定範囲の SPAN セッションを表示します。 <i>list</i> は有効なセッションの範囲です。 range は単一のセッション、または2つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 Note このキーワードは、特権 EXEC モードの場合だけ使用可能です。
remote	（任意）リモート SPAN セッションだけを表示します。
detail	（任意）指定されたセッションの詳細情報を表示します。

Command Modes

ユーザ EXEC
特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show monitor コマンドと **show monitor session all** コマンドの出力は同じです。

例

次に、**show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Device# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
Device# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
Device# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encaps : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encaps : Untagged
```

show monitor capture

モニタキャプチャ（WireShark）の内容を表示するには、特権 EXEC モードで **show monitor capture** コマンドを使用します。

```
show monitor capture [capture-name [ buffer ] | file file-location : file-name ][ brief | detailed | display-filter display-filter-string ]
```

Syntax Description					
<i>capture-name</i>	（任意）表示するキャプチャの名前を指定します。				
buffer	（任意）指定されたキャプチャに関連するバッファが表示されることを指定します。				
file <i>file-location</i> : <i>file-name</i>	（任意）表示するキャプチャストレージファイルのファイル位置と名前を指定します。				
brief	（任意）表示内容の概要を指定します。				
detailed	（任意）詳細な表示内容を指定します。				
display-filter <i>display-filter-string</i> <i>display-filter-string</i>	<i>display-filter-string</i> に従って表示内容をフィルタ処理します。				
Command Default	すべてのキャプチャの内容を表示します。				
Command Modes	特権 EXEC				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

例

次に、**show monitor capture** コマンドの出力例を示します。

```
Device# show monitor capture mycap

Status Information for Capture mycap
Target Type:
Interface: CAPWAP,
  Ingress:
0
  Egress:
0
Status : Active
Filter Details:
  Capture all packets
Buffer Details:
  Buffer Type: LINEAR (default)
File Details:
```

show monitor capture

```
Associated file name: flash:mycap.pcap
Size of buffer(in MB): 1
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packets per second: 0 (no limit)
Packet sampling rate: 0 (no sampling)
```

show parameter-map type subscriber attribute-to-service

パラメータマップの統計を表示するには、特権 EXEC モードで **show parameter-map type subscriber attribute-to-service** コマンドを使用します。

show parameter-map type subscriber attribute-to-service {all | name *parameter-map-name*}

Syntax Description	all	すべてのパラメータマップの統計を表示します。
	name <i>parameter-map-name</i>	指定したパラメータマップの統計を表示します。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Examples

次に、**show parameter-map type subscriber attribute-to-service name** *parameter-map-name* コマンドの出力例を示します。

```
Device# show parameter-map type subscriber attribute-to-service name platform

Parameter-map name: platform
Map: 10 platform-type regex "C9xxx"
Action(s):
  10 interface-template critical
```

show platform software fed switch ip wccp

プラットフォーム依存 Web Cache Communication Protocol (WCCP) 情報を表示するには、**show platform software fed switch ip wccp** 特権 EXEC コマンドを使用します。

```
show platform software fed switch {switch-number|active|standby}ip wccp
{cache-engines |interfaces |service-groups}
```

Syntax Description

switch {*switch_num* | **active** | **standby**} 情報を表示するデバイス。

- **switch_num**: スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。
- **active**: アクティブスイッチの情報を表示します。
- **standby**: 存在する場合、スタンバイスイッチの情報を表示します。

cache-engines WCCP キャッシュ エンジンを表示します。

interfaces WCCP インターフェイスを表示します。

service-groups WCCP サービス グループを表示します。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

このコマンドは、デバイスが IP サービスフィーチャセットを実行している場合だけ使用可能です。

次に、WCCP インターフェイスを表示する例を示します。

```
Device# show platform software fed switch 1 ip wccp interfaces
```

```
WCCP Interface Info
```

```
=====
```

```
**** WCCP Interface: Port-channel13 iif_id: 000000000000007c (#SG:3), VRF: 0 Ingress WCCP
****
port_handle:0x20000f9
```

```
List of Service Groups on this interface:
```

```
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).

* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).

* Service group id:60 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).

**** WCCP Interface: Port-channel14 iif_id: 000000000000007e (#SG:3), VRF: 0 Ingress WCCP
****
port_handle:0x880000fa

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).

* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).
<output truncated>
```

show platform software swspan

スイッチドポートアナライザ（SPAN）情報を表示するには、特権 EXEC モードで **show platform software swspan** コマンドを使用します。

```
show platform software swspan {switch} { {F0 | FP active} counters} | R0 | RP active}
{destination sess-id session-ID | source sess-id session-ID}
```

Syntax Description		
switch		スイッチに関する情報を表示します。
F0		Embedded Service Processor（ESP）スロット 0 に関する情報を表示します。
FP		ESP に関する情報を表示します。
active		ESP またはルート プロセッサ（RP）のアクティブ インスタンスに関する情報を表示します。
counters		SWSPAN メッセージ カウンタを表示します。
R0		RP スロット 0 に関する情報を表示します。
RP		RP に関する情報を表示します。
destination sess-id session-ID		指定された宛先セッションに関する情報を表示します。
source sess-id session-ID		指定された送信元セッションに関する情報を表示します。

Command Modes 特権 EXEC（#）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドは、Cisco IOS Release 16.1.1 よりも前のリリースで導入されました。

Usage Guidelines セッション番号が存在しないか、SPAN セッションがリモート接続先セッションの場合、コマンド出力には「% Error: No Information Available」のメッセージが表示されます。

Examples

次に、**show platform software swspan FP active source** コマンドの出力例を示します。

```
Switch# show platform software swspan FP active source sess-id 0

Showing SPAN source detail info

Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
Session Type : Local
```

```
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
AOM Object Status : Done
Parent AOM object Id : 118
Parent AOM object Status : Done
```

```
Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

次に、**show platform software swspan RP active destination** コマンドの出力例を示します。

```
Switch# show platform software swspan RP active destination
```

```
Showing SPAN destination table summary info
```

```
Sess-id IF-type IF-id Sess-type
-----
1 PORT 19 Remote
```

show flow exporter

フローエクスポートのステータスと統計情報を表示するには、特権 EXEC モードで **show flow exporter** コマンドを使用します。

show flow exporter [**broker** [**detail** | **picture**] | **export-ids netflow-v9** | [**name**] *exporter-name* [**statistics** | **templates**] | **statistics** | **templates**]

Syntax Description	
broker	(任意) Flexible NetFlow フローエクスポートのブローカの状態に関する情報を表示します。
detail	(任意) フローエクスポートのブローカに関する詳細な情報を表示します。
picture	(任意) ブローカ状態の画像を表示します。
export-ids netflow-v9	(任意) エクスポート可能な NetFlow バージョン 9 エクスポートフィールドとその ID を表示します。
name	(任意) フローエクスポートの名前を指定します。
<i>exporter-name</i>	(任意) 以前に設定されたフローエクスポートの名前。
statistics	(任意) すべてのフローエクスポートまたは指定されたフローエクスポートの統計情報を表示します。
templates	(任意) すべてのフローエクスポートまたは指定されたフローエクスポートのテンプレート情報を表示します。

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、デバイスで設定されているすべてのフローエクスポートのステータスと統計情報を表示する例を示します。

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:           Exports to the datacenter
  Export protocol:       NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:     192.168.0.2
    Transport Protocol:    UDP
    Destination Port:      9995
```

```

Source Port:          55864
DSCP:                0x0
TTL:                 255
Output Features:     Used

```

次の表で、この出力に表示される重要なフィールドについて説明します。

Table 105: show flow exporter のフィールドの説明

フィールド	説明
Flow Exporter	設定したフロー エクスポートの名前。
説明	エクスポートに設定した説明、またはユーザ定義のデフォルトの説明。
Transport Configuration	このエクスポートのトランスポート設定フィールド。
Destination IP address	宛先ホストの IP アドレス。
Source IP address	エクスポートされたパケットで使用される送信元 IP アドレス。
Transport Protocol	エクスポートされたパケットで使用されるトランスポート層プロトコル。
Destination Port	エクスポートされたパケットが送信される宛先 UDP ポート。
Source Port	エクスポートされたパケットが送信される送信元 UDP ポート。
DSCP	Differentiated Services Code Point (DSCP; DiffServ コードポイント) 値。
TTL	存続可能時間値。
Output Features	output-features コマンドが使用されたかどうかを指定します。このコマンドが使用されると、Flexible NetFlow エクスポート パケット上で出力機能が実行されます。

次に、デバイスで設定されているすべてのフローエクスポートのステータスと統計情報を表示する例を示します。

```

Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:          0                (0 bytes)

```

show flow interface

インターフェイスの Flexible NetFlow 設定およびステータスを表示するには、特権 EXEC モードで **show flow interface** コマンドを使用します。

show flow interface [*type number*]

Syntax Description	<i>type</i> (任意) Flexible NetFlow アカウンティング設定情報を表示するインターフェイスのタイプ。
	<i>number</i> (任意) Flexible NetFlow アカウンティング設定情報を表示するインターフェイスの番号。
Command Modes	特権 EXEC
Command History	リリース 変更内容 Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

Examples

次に、イーサネット インターフェイス 0/0 と 0/1 の Flexible NetFlow アカウンティング設定を表示する例を示します。

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
  monitor:          FLOW-MONITOR-1
  direction:       Output
  traffic(ip):      on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
  monitor:          FLOW-MONITOR-1
  direction:       Input
  traffic(ip):      sampler SAMPLER-2#
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 106: show flow interface のフィールドの説明

フィールド	説明
Interface	情報が適用されるインターフェイス。
monitor	インターフェイス上に設定されているフローモニタの名前。

フィールド	説明
direction:	フローモニタによってモニタされているトラフィックの方向。 次の値が可能です。 <ul style="list-style-type: none">• Input: インターフェイスが受信しているトラフィック。• Output: インターフェイスが送信しているトラフィック。
traffic(ip)	フローモニタが通常モードとサンプラーモードのどちらであることを示します。 次の値が可能です。 <ul style="list-style-type: none">• on: 通常モード。• sampler: サンプラーモード（サンプラーの名前も表示されます）。

show flow monitor

Flexible NetFlow フローモニタのステータスと統計情報を表示するには、特権 EXEC モードで **show flow monitor** コマンドを使用します。

show flow monitor [**broker** [**detail** | **picture**] | [**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] | **provisioning** | **statistics**]

Syntax Description

broker	(任意) フロー モニタのブローカの状態に関する情報を表示します。
detail	(任意) フロー モニタのブローカに関する詳細情報を表示します。
picture	(任意) ブローカ状態の画像を表示します。
name	(任意) フロー モニタの名前を指定します。
<i>monitor-name</i>	(任意) 事前に設定されたフロー モニタの名前。
cache	(任意) フロー モニタのキャッシュの内容を表示します。
format	(任意) ディスプレイ出力のフォーマットオプションのいずれかを使用することを指定します。
csv	(任意) フローモニタのキャッシュの内容をカンマ区切り値 (CSV) 形式で表示します。
record	(任意) フロー モニタのキャッシュの内容をレコード形式で表示します。
table	(任意) フロー モニタのキャッシュの内容を表形式で表示します。
provisioning	(任意) フロー モニタのプロビジョニング情報を表示します。
statistics	(任意) フロー モニタの統計情報を表示します。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

cache キーワードでは、デフォルトでレコード形式が使用されます。

show flowmonitor *monitor-name* **cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローの識別に Flexible NetFlow が使用するキーフィールドです。 **show flow monitor** *monitor-name* **cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、Flexible NetFlow がキャッシュの追加データとして値を収集する非キーフィールドです。

Examples

次の例では、フロー モニタのステータスを表示します。

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:     flow-record-1
  Flow Exporter:   flow-exporter-1
                  flow-exporter-2

  Cache:
    Type:           normal
    Status:         allocated
    Size:           4096 entries / 311316 bytes
    Inactive Timeout: 15 secs
    Active Timeout: 1800 secs
    Update Timeout: 1800 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 107: show flow monitor monitor-name フィールドの説明

フィールド	説明
Flow Monitor	設定したフロー モニタの名前。
説明	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
Flow Record	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フロー モニタに割り当てられたエクスポータ。
Cache	フロー モニタのキャッシュに関する情報。
Type	フロー モニタのキャッシュ タイプ。 次の値が可能です。 <ul style="list-style-type: none"> • immediate: フローは即座に期限切れになります。 • normal: フローは通常どおり期限切れになります。 • Permanent: フローは期限切れになりません。
Status	フロー モニタのキャッシュのステータス。 次の値が可能です。 <ul style="list-style-type: none"> • allocated: キャッシュが割り当てられています。 • being deleted: キャッシュが削除されています。 • not allocated: キャッシュが割り当てられていません。
Size	現在のキャッシュ サイズ。

フィールド	説明
Inactive Timeout	非アクティブ タイムアウトの現在の値（秒単位）。
Active Timeout	アクティブ タイムアウトの現在の値（秒単位）。
Update Timeout	更新タイムアウトの現在の値（秒単位）。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表示します。

```

Device# show flow monitor FLOW-MONITOR-1 cache
Cache type:                               Normal (Platform cache)
Cache size:                               Unknown
Current entries:                           1

Flows added:                               3
Flows aged:                                2
  - Active timeout      ( 300 secs)        2

DATALINK MAC SOURCE ADDRESS INPUT:         0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:    6400.F125.59E6
IPV6 SOURCE ADDRESS:                       2001:DB8::1
IPV6 DESTINATION ADDRESS:                  2001:DB8:1::1
TRNS SOURCE PORT:                          1111
TRNS DESTINATION PORT:                     2222
IP VERSION:                                6
IP PROTOCOL:                               6
IP TOS:                                    0x05
IP TTL:                                    11
tcp flags:                                  0x20
counter bytes long:                         132059538
counter packets long:                       1158417

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 108: show flow monitor monitor-name cache フィールドの説明

フィールド	説明
Cache type	フローモニタのキャッシュタイプ。この値は常に normal となります。これが唯一サポートされているキャッシュタイプです。
Cache Size	キャッシュ内のエントリ数。
Current entries	キャッシュ内の使用中のエントリ数。
Flows added	キャッシュの作成後にキャッシュに追加されたフロー。
Flows aged	キャッシュの作成後に期限切れになったフロー。
Active timeout	アクティブ タイムアウトの現在の値（秒単位）。
Inactive timeout	非アクティブ タイムアウトの現在の値（秒単位）。

フィールド	説明
DATALINK MAC SOURCE ADDRESS INPUT	入力パケットの MAC 送信元アドレス。
DATALINK MAC DESTINATION ADDRESS INPUT	入力パケットの MAC 宛先アドレス。
IPV6 SOURCE ADDRESS	IPv6 送信元アドレスです。
IPV6 DESTINATION ADDRESS	IPv6 宛先アドレス。
TRNS SOURCE PORT	トランスポートプロトコルの送信元ポート。
TRNS DESTINATION PORT	トランスポートプロトコルの宛先ポート。
IP VERSION	IP バージョン。
IP PROTOCOL	プロトコル番号。
IP TOS	IP タイプ オブ サービス (ToS) の値。
IP TTL	IP 存続可能時間 (TTL) の値。
tcp flags	TCP フラグの値。
counter bytes	カウントされたバイト数。
counter packets	カウントされたパケット数。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表形式で表示します。

```

Device# show flow monitor FLOW-MONITOR-1 cache format table
Cache type:                Normal (Platform cache)
Cache size:                 Unknown
Current entries:           1

Flows added:                3
Flows aged:                 2
  - Active timeout        ( 300 secs)  2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes long
pkts long
=====
=====
=====
0000.0000.1000                6400.F125.59E6                2001:DB8::1    2001:DB8:1::1
      1111                2222                6                6 0x05                11 0x20                132059538
1158417
    
```

次の例では、FLOW-MONITOR-IPv6 という名前のフロー モニタ (キャッシュに IPv6 データを格納) のステータス、統計情報、およびデータをレコード形式で表示します。

```
Device# show flow monitor name FLOW-MONITOR-IPv6 cache format record
Cache type:                               Normal (Platform cache)
Cache size:                               Unknown
Current entries:                           1

Flows added:                               3
Flows aged:                               2
  - Active timeout      ( 300 secs)       2

DATALINK MAC SOURCE ADDRESS INPUT:         0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:    6400.F125.59E6
IPV6 SOURCE ADDRESS:                       2001::2
IPV6 DESTINATION ADDRESS:                  2002::2
TRNS SOURCE PORT:                          1111
TRNS DESTINATION PORT:                     2222
IP VERSION:                                6
IP PROTOCOL:                               6
IP TOS:                                    0x05
IP TTL:                                    11
tcp flags:                                 0x20
counter bytes long:                        132059538
counter packets long:                      1158417
```

次の例では、フローモニタのステータスと統計情報を表示します。

```
Device# show flow monitor FLOW-MONITOR-1 statistics
Cache type:                               Normal (Platform cache)
Cache size:                               Unknown
Current entries:                           1

Flows added:                               3
Flows aged:                               2
  - Active timeout      ( 300 secs)       2
```

show flow record

Flexible NetFlow フローレコードのステータスと統計情報を表示するには、特権 EXEC モードで **show flow record** コマンドを使用します。

```
show flow record [broker [detail | picture]] [[name] record-name]
```

Syntax Description	broker (任意) Flexible NetFlow フローレコードのブローカの状態に関する情報を表示します。				
	detail (任意) フローレコードのブローカに関する詳細な情報を表示します。				
	picture (任意) ブローカ状態の画像を表示します。				
	name (任意) フローレコードの名前を指定します。				
	record-name (任意) 前に設定されたユーザ定義のフローレコードの名前。				
Command Default	なし				
Command Modes	特権 EXEC				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

次に、FLOW-RECORD-1 のステータスおよび統計情報を表示する例を示します。

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:      User defined
  No. of users:    0
  Total field space: 24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

show sampler

Flexible NetFlow サンプラーのステータスと統計情報を表示するには、特権 EXEC モードで **show sampler** コマンドを使用します。

show sampler [**broker** [**detail** | **picture**] | [**name**] *sampler-name*]

Syntax Description	
broker	(任意) Flexible NetFlow サンプラーのブローカのステータスに関する情報を表示します。
detail	(任意) サンプラーのブローカに関する詳細な情報を表示します。
picture	(任意) ブローカ状態の画像を表示します。
name	(任意) サンプラーの名前を指定します。
<i>sampler-name</i>	(任意) 前に設定されたサンプラーの名前。

Command Default なし

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、設定されたフロー サンプラーすべてのステータスと統計情報を表示する例を示します。

```
Device# show sampler
Sampler SAMPLER-1:
  ID:                2083940135
  export ID:         0
  Description:       User defined
  Type:              Invalid (not in use)
  Rate:              1 out of 32
  Samples:           0
  Requests:          0
  Users (0):

Sampler SAMPLER-2:
  ID:                3800923489
  export ID:         1
  Description:       User defined
  Type:              random
  Rate:              1 out of 100
  Samples:           1
  Requests:          124
  Users (1):
    flow monitor FLOW-MONITOR-1 (datalink,vlan1) 0 out of 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 109: show sampler のフィールドの説明

フィールド	説明
ID	フロー サンプラーの ID 番号。
Export ID	フロー サンプラーのエクスポートの ID。
説明	フローサンプラーに設定した説明、またはユーザ定義のデフォルトの説明。
Type	フローサンプラーに設定したサンプリングモード。
Rate	フロー サンプラーに設定したウィンドウ サイズ (パケットの選択用)。指定できる範囲は 2 ~ 32768 です。
Samples	フローサンプラーを設定してから、またはデバイスを再起動してからサンプリングされたパケットの数。この数は、トラフィックのサンプリングが必要かどうかを決定するためにサンプラーが呼び出されたときに肯定応答を受信した回数と同じです。この表の Requests フィールドの説明を参照してください。
Requests	トラフィックのサンプリングが必要かどうかを決定するためにサンプラーが呼び出された回数。
Users	フローサンプラーが設定されるインターフェイス。

show snmp stats

SNMP の統計を表示するには、特権 EXEC モードで **show snmp stats** コマンドを使用します。

```
show snmp stats { hosts | oid }
```

Syntax Description

hosts SNMP エージェントにポーリングされた SNMP サーバの詳細を表示します。

oid 最近要求されたオブジェクト識別子 (OID) を表示します。

Command Default

SNMP エージェントにポーリングされた SNMP マネージャエントリを表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines

show snmp stats hosts コマンドは、NMS の IP アドレス、NMS がエージェントをポーリングした回数、およびポーリングのタイムスタンプを一覧表示するために使用します。SNMP エージェントにポーリングされたエントリを削除するには、**clear snmp stats hosts** コマンドを使用します。

show snmp stats oid コマンドを実行する前に、デバイスを NMS に接続します。コマンド出力には、NMS から最近要求された OID のリストが表示されます。また、オブジェクト ID が NMS から要求された回数も示します。この情報は、NMS が照会している MIB に関する情報がほとんどない場合に、メモリリークやネットワーク障害のトラブルシューティングに役立ちます。**show snmp stats oid** コマンドを使用すると、NMS から最近要求された OID をいつでも確認できます。

次に、**show snmp stats hosts** コマンドの出力例を示します。

```
Device# show snmp stats hosts
Request Count      Last Timestamp      Address
2                  00:00:01 ago        3.3.3.3
1                  1w2d ago            2.2.2.2
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 110: show snmp stats hosts のフィールドの説明

フィールド	説明
Request Count	SNMP マネージャから SNMP エージェントに要求が送信された回数が表示されます。
Last Timestamp	SNMP マネージャから SNMP エージェントに要求が送信された時刻が表示されます。

フィールド	説明
Address	要求を送信した SNMP マネージャの IP アドレスが表示されます。

次に、**show snmp stats oid** コマンドの出力例を示します。

Device# **show snmp stats oid**

```

time-stamp                #of times requested      OID
15:30:01 UTC Dec 2 2019      6      ifPhysAddress
15:30:01 UTC Dec 2 2019     10      system.2
15:30:01 UTC Dec 2 2019      9      system.1
09:39:39 UTC Nov 26 2019      3      system.5
09:39:39 UTC Nov 26 2019      3      stem.4
09:39:39 UTC Nov 26 2019      3      system.7
09:39:39 UTC Nov 26 2019      2      system.6
09:39:39 UTC Nov 26 2019     10      ceemEventMapEntry.2
09:39:39 UTC Nov 26 2019      6      ipAddrEntry.4
09:39:39 UTC Nov 26 2019      3      ipAddrEntry.5
09:39:39 UTC Nov 26 2019     10      ipAddrEntry.3
09:39:39 UTC Nov 26 2019      7      ipAddrEntry.2
09:39:39 UTC Nov 26 2019      4      ipAddrEntry.1
09:39:39 UTC Nov 26 2019      1      lsystem.3

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 111: show snmp stats oid のフィールドの説明

フィールド	説明
time-stamp	NMS からオブジェクト識別子が要求された日時が表示されます。
#of times requested	オブジェクト ID が要求された回数を表示します。
OID	NMS から最近要求されたオブジェクト識別子が表示されます。

snmp ifmib ifindex persist

維持させる ifIndex 値をグローバルにイネーブルにし、リポート後も維持されるようにして、Simple Network Management Protocol (SNMP) で使用できるようにするには、グローバル コンフィギュレーション モードで **snmp ifmib ifindex persist** コマンドを使用します。ifIndex パーシステンスをグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp ifmib ifindex persist
no snmp ifmib ifindex persist

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

デバイスの ifIndex パーシステンスがディセーブルになります。

Command Modes

グローバル コンフィギュレーション (config)

Usage Guidelines

snmp ifmib ifindex persist コマンドは、インターフェイス固有の設定をオーバーライドしません。ifIndex パーシステンスのインターフェイス固有の設定は、インターフェイス コンフィギュレーション モードで **snmp ifindex persist** コマンドと **snmp ifindex clear** コマンドを使用して設定されます。

snmp ifmib ifindex persist コマンドは、インターフェイス MIB (IF-MIB) の ifIndex テーブル内の ifDescr エントリと ifIndex エントリを使用して、ルーティングデバイス上のすべてのインターフェイスの ifIndex パーシステンスをイネーブルにします。

ifIndex パーシステンスとは、リポート後も IF-MIB 内の ifIndex 値を存続させ、SNMP を使用する特定のインターフェイスの ID が維持されるようにします。

ifIndex パーシステンスが **no snmp ifindex persist** コマンドを使用して、特定のインターフェイスに対して以前にディセーブルされていた場合、ifIndex パーシステンスはそのインターフェイスではディセーブルのままとなります。

Examples

次に、すべてのインターフェイスの ifIndex パーシステンスをイネーブルにする例を示します。

```
Device(config)# snmp ifmib ifindex persist
```

Related Commands

コマンド	説明
snmp ifindex clear	以前に特定のインターフェイスに対してインターフェイス コンフィギュレーション モードで発行された設定済み snmp ifIndex コマンドをクリアします。
snmp ifindex persist	IF-MIB でリポート後も維持する (ifIndex persistence) ifIndex 値をイネーブルにします。

snmp-server community

Simple Network Management Protocol (SNMP) へのアクセスを許可するコミュニティ アクセスストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。指定したコミュニティストリングを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server community [clear | encrypted] community-string [view
view-name] [RO | RW] [SDROwner | SystemOwner] [access-list-name]
no snmp-server community community-string
```

Syntax Description

clear	(任意) 入力された <i>community-string</i> がクリアテキストで、 show running コマンドで表示されるときに暗号化されるように指定します。
encrypted	(任意) 入力された <i>community-string</i> が暗号化テキストで、 show running コマンドの実行時に暗号化されて表示されるように指定します。
<i>community-string</i>	パスワードのように動作し、SNMP プロトコルへのアクセスを許可します。 <i>community-string</i> 引数の最大長は 32 文字の英字です。 clear キーワードが使用された場合、 <i>community-string</i> はクリアテキストと見なされます。 encrypted キーワードが使用された場合、 <i>community-string</i> は暗号化テキストと見なされます。どちらも使用されなかった場合、 <i>community-string</i> はクリアテキストと見なされます。
view <i>view-name</i>	(任意) 事前に定義したビューの名前を指定します。ビューには、コミュニティで使用できるオブジェクトが定義されています。
RO	(任意) 読み取り専用アクセス権を指定します。許可された管理ステーションは、MIB オブジェクトの取得だけを実行できます。
RW	(任意) 読み取り/書き込みアクセス権を指定します。許可された管理ステーションは、MIB オブジェクトの取得と修正の両方を実行できます。
SDROwner	(任意) オーナー Service Domain Router (SDR) へのアクセスを制限します。
SystemOwner	(任意) オーナー以外のすべての SDR へのアクセスを含むシステム全体へのアクセスを提供します。
<i>access-list-name</i>	(任意) SNMP エージェントへアクセスするためにコミュニティストリングの使用を許可された IP アドレスのアクセスリスト名。

Command Default

SNMP コミュニティストリングは、デフォルトで、すべての MIB オブジェクトへの読み取り専用アクセスを許可しています。コミュニティストリングは、デフォルトで、SDR オーナーに割り当てられます。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Usage Guidelines

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザーグループに属している必要があります。ユーザーグループの割り当てが原因でコマンドを使用できない場合、AAA 管理者に連絡してください。

コミュニティ アクセス スtring を設定して SNMP へのアクセスを許可するには、**snmp-server community** コマンドを使用します。

指定したコミュニティ スtring を削除するには、このコマンドの **no** 形式を使用します。

クリアテキストで入力したコミュニティ スtring を **show running** コマンドの出力で暗号化して表示するには、**clear** キーワードを使用します。暗号化された String を入力するには、**encrypted** キーワードを使用します。クリアテキストでコミュニティ スtring を入力し、それがシステムによって暗号化されないようにするには、どちらのキーワードも使用しないようにします。

SDROwner キーワードを指定して **snmp-server community** コマンドを入力すると、オーナー SDR 内の MIB オブジェクトインスタンスに対してのみ SNMP アクセスが許可されます。**SystemOwner** キーワードを指定して **snmp-server community** コマンドを入力すると、システム内のすべての SDR に SNMP アクセスが許可されます。



Note オーナー以外の SDR では、コミュニティ名は、そのコミュニティ名に割り当てられたアクセス権限に関係なく、その SDR に属するオブジェクトインスタンスだけにアクセスを許可します。オーナー SDR へのアクセスおよびシステム全体のアクセス特権は、オーナー SDR からだけ使用できます。

Examples

次に、**comaccess** スtring を SNMP に割り当てて読み取り専用アクセスを許可する方法、および IP アクセス リスト 4 がコミュニティ スtring を使用できるように指定する例を示します。

```
RP/0/RP0/CPU0:router(config)# snmp-server community comaccess ro 4
```

次に、**mgr** スtring を SNMP に割り当てて、制限ビューのオブジェクトへの読み取りと書き込みアクセスを許可する例を示します。

```
RP/0/RP0/CPU0:router(config)# snmp-server community mgr view restricted rw
```

次に、**comaccess** コミュニティを削除する例を示します。

```
RP/0/RP0/CPU0:router(config)# no snmp-server community comaccess
```

Related Commands

コマンド	説明
snmp-server view	SNMP のビュー エントリを作成または更新します。

snmp-server enable traps

デバイスでネットワーク管理システム（NMS）にインフォーム要求やさまざまなトラップの Simple Network Management Protocol（SNMP）通知を送信可能にするには、グローバルコンフィギュレーションモードで **snmp-server enable traps** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

no snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

Syntax Description	
auth-framework	（任意）SNMP CISCO-AUTH-FRAMEWORK-MIB トラップをイネーブルにします。
sec-violation	（任意）SNMP camSecurityViolationNotif 通知をイネーブルにします。
bridge	（任意）SNMP STP ブリッジ MIB トラップをイネーブルにします。*
call-home	（任意）SNMP CISCO-CALLHOME-MIB トラップをイネーブルにします。*
config	（任意）SNMP 設定トラップをイネーブルにします。
config-copy	（任意）SNMP 設定コピートラップをイネーブルにします。
config-ctid	（任意）SNMP 設定 CTID トラップをイネーブルにします。
copy-config	（任意）SNMP コピー設定トラップをイネーブルにします。
cpu	（任意）CPU 通知トラップをイネーブルにします。*
dot1x	（任意）SNMP dot1x トラップをイネーブルにします。*
energywise	（任意）SNMP energywise トラップをイネーブルにします。 *

entity	(任意) SNMP エンティティ トラップをイネーブルにします。
envmon	(任意) SNMP 環境モニタ トラップをイネーブルにします。 *
errdisable	(任意) SNMP エラーディセーブルトラップをイネーブルにします。*
event-manager	(任意) SNMP 組み込みイベント マネージャ トラップをイネーブルにします。
flash	(任意) SNMP フラッシュ通知トラップをイネーブルにします。*
fru-ctrl	(任意) エンティティ現場交換可能ユニット (FRU) 制御トラップを生成します。デバイススタックでは、このトラップはスタックにおけるデバイスの挿入/取り外しを意味します。
license	(任意) ライセンストラップをイネーブルにします。*
mac-notification	(任意) SNMP MAC 通知トラップをイネーブルにします。*
port-security	(任意) SNMP ポートセキュリティトラップをイネーブルにします。*
power-ethernet	(任意) SNMP パワーイーサネットトラップをイネーブルにします。*
rep	(任意) SNMP レジリエントイーサネットプロトコルトラップをイネーブルにします。
snmp	(任意) SNMP トラップをイネーブルにします。*
stackwise	(任意) SNMP StackWise トラップをイネーブルにします。*
storm-control	(任意) SNMP ストーム制御トラップパラメータをイネーブルにします。
stpx	(任意) SNMP STPX MIB トラップをイネーブルにします。 *
syslog	(任意) SNMP syslog トラップをイネーブルにします。
transceiver	(任意) SNMP トランシーバトラップをイネーブルにします。*
tty	(任意) TCP 接続トラップを送信します。この設定はデフォルトでイネーブルになっています。

vlan-membership	(任意) SNMP VLAN メンバーシップ トラップをイネーブルにします。
vlancreate	(任意) SNMP VLAN 作成トラップをイネーブルにします。
vlandelete	(任意) SNMP VLAN 削除トラップをイネーブルにします。
vstack	(任意) SNMP スマートインストールトラップをイネーブルにします。*
vtp	(任意) VLAN トランキンングプロトコル (VTP) トラップをイネーブルにします。

Command Default SNMP トラップの送信をディセーブルにします。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 上記の表のアスタリスクが付いているコマンドオプションにはサブコマンドがあります。これらのサブコマンドの詳細については、関連コマンドの項を参照してください。

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。

トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにするには、**snmp-server enable traps** コマンドを使用します。



Note **fru-ctrl, insertion** および **removal** キーワードは、コマンドラインのヘルプストリングに表示されませんが、デバイスでサポートされていません。**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host host-addr informs** グローバル コンフィギュレーション コマンドを組み合わせ使用します。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、複数の SNMP トラップ タイプをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps config  
Device(config)# snmp-server enable traps vtp
```

snmp-server enable traps bridge

STPブリッジMIBトラップを生成するには、グローバルコンフィギュレーションモードで **snmp-server enable traps bridge** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps bridge [newroot] [topologychange]
no snmp-server enable traps bridge [newroot] [topologychange]
```

Syntax Description	newroot (任意) SNMP STPブリッジMIB新規ルートトラップをイネーブルにします。				
	topologychange (任意) SNMP STPブリッジMIBトポロジ変更トラップをイネーブルにします。				
Command Default	ブリッジSNMPトラップの送信はディセーブルになります。				
Command Modes	グローバルコンフィギュレーション				
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Fuji 16.9.2</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines **snmp-server host** グローバルコンフィギュレーションコマンドを使用して、トラップを受信するホスト(NMS)を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次の例では、NMSにブリッジ新規ルートトラップを送信する方法を示します。

```
Device(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

データ収集 MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps bulkstat** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps bulkstat [collection | transfer]
no snmp-server enable traps bulkstat [collection | transfer]

Syntax Description

collection (任意) データ収集 MIB 収集トラップをイネーブルにします。

transfer (任意) データ収集 MIB 送信トラップをイネーブルにします。

Command Default

データ収集 MIB トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、データ収集 MIB 収集トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

SNMP CISCO-CALLHOME-MIB トラップをイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps call-home** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps call-home [**message-send-fail** | **server-fail**]
no snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

Syntax Description

message-send-fail (任意) SNMP メッセージ送信失敗トラップをイネーブルにします。

server-fail (任意) SNMP サーバ障害トラップをイネーブルにします。

Command Default

SNMP CISCO-CALLHOME-MIB トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、SNMP メッセージ送信失敗トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

SNMP Cisco Express Forwarding (CEF) トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps cef** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

Syntax Description	
inconsistency	(任意) SNMP CEF 矛盾トラップをイネーブルにします。
peer-fib-state-change	(任意) SNMP CEF ピア FIB ステート変更トラップをイネーブルにします。
peer-state-change	(任意) SNMP CEF ピア ステート変更トラップをイネーブルにします。
resource-failure	(任意) SNMP リソース障害トラップをイネーブルにします。

Command Default SNMP CEF トラップの送信はディセーブルになります。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、SNMP CEF 矛盾トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps envmon

SNMP 環境トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps envmon** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps envmon [ status ]
no snmp-server enable traps envmon [ status ]
```

Syntax Description

status (任意) SNMP 環境ステータス変更トラップをイネーブルにします。

Command Default

環境 SNMP トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server enable traps envmon status コマンドは、環境ステータス変更トラップに加えて、ファン、電源、および温度のトラップもイネーブルにします。

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、ステータス変更トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps envmon status
```

snmp-server enable traps errdisable

エラーディセーブルの SNMP 通知をイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps errdisable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]
no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

Syntax Description	notification-rate <i>number-of-notifications</i>	(任意) 通知レートとして 1 分当たりの通知の数を指定します。受け入れられる値の範囲は 0 ~ 10000 です。
---------------------------	--	--

Command Default	エラー ディセーブルの SNMP 通知送信はディセーブルになります。
------------------------	------------------------------------

Command Modes	グローバル コンフィギュレーション
----------------------	-------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。
-------------------------	--



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、エラー ディセーブルの SNMP 通知数を 2 に設定する例を示します。

```
Device(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

SNMP フラッシュ通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps flash** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps flash [insertion] [removal]
no snmp-server enable traps flash [insertion] [removal]

Syntax Description

insertion (任意) SNMP フラッシュ挿入通知をイネーブルにします。

removal (任意) SNMP フラッシュ取り出し通知をイネーブルにします。

Command Default

SNMP フラッシュ通知の送信はディセーブルです。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、SNMP フラッシュ挿入通知を生成する例を示します。

```
Device(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps isis

Intermediate System-to-Intermediate System (IS-IS) リンクステートルーティングプロトコルトラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps isis** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps isis [errors | state-change]
no snmp-server enable traps isis [errors | state-change]
```

Syntax Description

errors (任意) IS-IS エラー トラップをイネーブルにします。

state-change (任意) IS-IS ステート変更トラップをイネーブルにします。

Command Default

IS-IS のトラップ送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、IS-IS エラー トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

ライセンストラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps license** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps license [deploy] [error] [usage]
no snmp-server enable traps license [deploy] [error] [usage]
```

Syntax Description

deploy (任意) ライセンス導入トラップをイネーブルにします。

error (任意) ライセンスエラートラップをイネーブルにします。

usage (任意) ライセンス使用トラップをイネーブルにします。

Command Default

ライセンストラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、ライセンス導入トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

SNMP MAC 通知トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps mac-notification** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]
no snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]

Syntax Description

change (任意) SNMP MAC 変更トラップをイネーブルにします。

move (任意) SNMP MAC 移動トラップをイネーブルにします。

threshold (任意) SNMP MAC しきい値トラップをイネーブルにします。

Command Default

SNMP MAC 通知トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、SNMP MAC 通知変更トラップを生成する例を示します。

```
Device (config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

SNMP の Open Shortest Path First (OSPF) トラップをイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps ospf** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps ospf [cisco-specific | errors | lsa | rate-limit rate-limit-time
max-number-of-traps | retransmit | state-change]
no snmp-server enable traps ospf [cisco-specific | errors | lsa | rate-limit rate-limit-time
max-number-of-traps | retransmit | state-change]
```

Syntax Description	
cisco-specific	(任意) シスコ固有のトラップをイネーブルにします。
errors	(任意) エラー トラップをイネーブルにします。
lsa	(任意) リンクステートアドバタイズメント (LSA) トラップをイネーブルにします。
rate-limit	(任意) レート制限トラップをイネーブルにします。
<i>rate-limit-time</i>	(任意) レート制限トラップの時間の長さを秒数で指定します。指定できる値は 2 ~ 60 です。
<i>max-number-of-traps</i>	(任意) 設定した時間内に送信するレート制限トラップの最大数を指定します。
retransmit	(任意) パケット再送信トラップをイネーブルにします。
state-change	(任意) 状態変更トラップをイネーブルにします。

Command Default OSPF SNMP トラップの送信はディセーブルになります。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、LSA トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

SNMP プロトコル独立型マルチキャスト（PIM）トラップをイネーブルにするには、グローバル コンフィギュレーションモードで **snmp-server enable traps pim** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps pim [invalid-pim-message] [neighbor-change] [rp-mapping-change]
no snmp-server enable traps pim [invalid-pim-message] [neighbor-change] [rp-mapping-change]
```

Syntax Description

invalid-pim-message （任意）無効な PIM メッセージトラップをイネーブルにします。

neighbor-change （任意）PIM ネイバー変更トラップをイネーブルにします。

rp-mapping-change （任意）ランデブーポイント（RP）マッピング変更トラップをイネーブルにします。

Command Default

PIM SNMP トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、無効な PIM メッセージトラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

SNMP ポートセキュリティトラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps port-security** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps port-security [**trap-rate** *value*]
no snmp-server enable traps port-security [**trap-rate** *value*]

Syntax Description	trap-rate <i>value</i>	(任意) 1 秒間に送信するポートセキュリティトラップの最大数を設定します。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 です (制限はなく、トラップは発生するたびに送信されます)。
Command Default	ポートセキュリティ SNMP トラップの送信はディセーブルになります。	
Command Modes	グローバル コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、1 秒当たり 200 の速度でポートセキュリティトラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

SNMP の Power over Ethernet (PoE) トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps power-ethernet** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps power-ethernet {group number | police}
no snmp-server enable traps power-ethernet {group number | police}
```

Syntax Description	group number	指定したグループ番号に対するインライン パワー グループベース トラップをイネーブルにします。受け入れられる値の範囲は 1 ~ 9 です。
	police	インライン パワー ポリシング トラップをイネーブルにします。

Command Default Power over Ethernet の SNMP トラップの送信はディセーブルになります。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、グループ 1 の Power over Ethernet (PoE) トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps poower-over-ethernet group 1
```

snmp-server enable traps snmp

SNMP トラップをイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps snmp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup] [warmstart]
no snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup] [warmstart]
```

Syntax Description

authentication	(任意) 認証トラップをイネーブルにします。
coldstart	(任意) コールドスタートトラップをイネーブルにします。
linkdown	(任意) リンクダウントラップをイネーブルにします。
linkup	(任意) リンクアップトラップをイネーブルにします。
warmstart	(任意) ウォームスタートトラップをイネーブルにします。

Command Default

SNMP トラップの送信をディセーブルにします。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、ウォーム スタートの SNMP トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps storm-control

SNMP ストーム制御トラップパラメータをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps storm-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps storm-control { trap-rate number-of-minutes }  
no snmp-server enable traps storm-control { trap-rate }
```

Syntax Description	trap-rate <i>number-of-minutes</i>	(任意) SNMP ストーム制御トラップ レートを分単位で指定します。受け入れられる値の範囲は 0 ~ 1000 です。デフォルトは 0 です。 値 0 は、制限が適用されず、発生するたびにトラップが送信されることを示します。設定すると、 show run all コマンド出力に no snmp-server enable traps storm-control が表示されます。
Command Default	SNMP ストーム制御トラップ パラメータの送信はディセーブルになります。	
Command Modes	グローバル コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。	



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、SNMP ストーム制御トラップレートを 1 分あたり 10 トラップに設定する例を示します。

```
Device(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

SNMP STPX MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps stpx** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]
no snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]
```

Syntax Description

inconsistency (任意) SNMP STPX MIB 矛盾更新トラップをイネーブルにします。

loop-inconsistency (任意) SNMP STPX MIB ループ矛盾更新トラップをイネーブルにします。

root-inconsistency (任意) SNMP STPX MIB ルート矛盾更新トラップをイネーブルにします。

Command Default

SNMP STPX MIB トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、SNMP STPX MIB 矛盾更新トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

SNMP トランシーバトラップをイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps transceiver** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps transceiver {all}
no snmp-server enable traps transceiver {all}
```

Syntax Description

all (任意) すべての SNMP トランシーバトラップをイネーブルにします。

Command Default

SNMP トランシーバトラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、すべての SNMP トランシーバトラップを設定する例を示します。

```
Device(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

SNMP vrfmib トラップを許可するには、グローバルコンフィギュレーションモードで **snmp-server enable traps vrfmib** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vrfmib [vnet-trunk-down | vnet-trunk-up | vrf-down | vrf-up]
no snmp-server enable traps vrfmib [vnet-trunk-down | vnet-trunk-up | vrf-down | vrf-up]

Syntax Description

vnet-trunk-down (任意) vrfmib trunk ダウントラップをイネーブルにします。

vnet-trunk-up (任意) vrfmib trunk アップトラップをイネーブルにします。

vrf-down (任意) vrfmib vrf ダウントラップをイネーブルにします。

vrf-up (任意) vrfmib vrf アップトラップをイネーブルにします。

Command Default

SNMP vrfmib トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

この例は、vrfmib trunk ダウントラップを生成する方法を示しています。

```
Device(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

SNMP スマート インストール トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps vstack** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vstack [addition] [failure] [lost] [operation]
no snmp-server enable traps vstack [addition] [failure] [lost] [operation]

Syntax Description

addition (任意) クライアントによって追加されたトラップをイネーブルにします。

failure (任意) ファイルのアップロードとダウンロード障害トラップをイネーブルにします。

lost (任意) クライアントの損失トラップをイネーブルにします。

operation (任意) 動作モード変更トラップをイネーブルにします。

Command Default

SNMP スマート インストール トラップの送信はディセーブルになります。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



Note SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

Examples

次に、SNMP スマートインストールクライアント追加トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps vstack addition
```

snmp-server engineID

SNMP のローカルコピーまたはリモートコピーに名前を設定するには、グローバル コンフィギュレーション モードで **snmp-server engineID** コマンドを使用します。

snmp-server engineID {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*]
engineid-string}

Syntax Description	local <i>engineid-string</i>	remote <i>ip-address</i>	udp-port <i>port-number</i>
	SNMP コピーの名前に 24 文字の ID 文字列を指定します。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。	リモート SNMP コピーを指定します。SNMP のリモート コピーを含むデバイスの <i>ip-address</i> を指定します。	(任意) リモート デバイスのユーザ データグラム プロトコル (UDP) ポートを指定します。デフォルトは 162 です。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines なし

例

次の例では、ローカル エンジン ID 12340000000000000000000000000000 を設定します。

```
Device(config)# snmp-server engineID local 1234
```

snmp-server group

新しい Simple Network Management Protocol (SNMP) グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP グループを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server group group-name {v1|v2c|v3 {auth|noauth|priv}} [context context-name] [match {exact|prefix}] [read read-view] [write write-view] [notify notify-view] [access [ipv6 named-access-list] [acl-numberacl-name]]
```

```
no snmp-server group group-name {v1|v2c|v3 {auth|noauth|priv}} [context context-name]
```

Syntax Description

<i>group-name</i>	グループの名前。
v1	グループが SNMPv1 セキュリティ モデルを使用していることを指定します。SNMPv1 は、最も安全性の低い SNMP セキュリティ モデルです。
v2c	グループが SNMPv2c セキュリティ モデルを使用していることを指定します。SNMPv2c セキュリティ モデルでは、インフォームを送信でき、64 文字の文字列がサポートされています。
v3	グループが SNMPv3 セキュリティ モデルを使用していることを指定します。SNMPv3 は、サポートされているセキュリティ モデルの中で最も安全です。SNMPv3 では、認証特性を明示的に設定できます。
auth	暗号化を行わないパケットの認証を指定します。
noauth	パケットの認証を行わないことを指定します。
priv	暗号化を行うパケットの認証を指定します。
context	(任意) この SNMP グループとそのビューと関連付ける SNMP コンテキストを指定します。
<i>context-name</i>	(任意) コンテキスト名。
match	(任意) 正確なコンテキスト マッチを指定するか、またはコンテキストプレフィックスのみを照合します。
<i>exact</i>	(任意) 正確なコンテキストを照合します。
<i>prefix</i>	(任意) コンテキストプレフィックスのみを照合します。
read	(任意) SNMP グループの読み取りビューを指定します。このビューでは、エージェントのコンテンツのみを表示できます。

<i>read-view</i>	<p>(任意) ビューの名前である最大 64 文字の文字列。</p> <p>デフォルトでは、read オプションを使用してこの状態を上書きしない限り、読み取りビューはインターネットオブジェクト識別子 (OID) のスペース (1.3.6.1) に属するすべてのオブジェクトであるとみなされます。</p>
write	<p>(任意) SNMP グループの書き込みビューを指定します。このビューでは、データを入力してエージェントのコンテンツを設定できます。</p>
<i>write-view</i>	<p>(任意) ビューの名前である最大 64 文字の文字列。</p> <p>デフォルトでは、書き込みビュー (つまり、ヌル OID) には何も定義されていません。書き込みアクセスを設定する必要があります。</p>
notify	<p>(任意) SNMP グループの通知ビューを指定します。このビューでは、通知、インフォーム、またはトラップを指定できます。</p>
<i>notify-view</i>	<p>(任意) ビューの名前である最大 64 文字の文字列。</p> <p>デフォルトでは、snmp-server host コマンドが設定されるまで、通知ビュー (つまり、ヌル OID) には何も定義されていません。ビューを snmp-server group コマンドで指定した場合、生成されるそのビューのすべての通知は、グループに関連付けられているすべてのユーザに送信されます (そのユーザに対して SNMP サーバホストの設定が存在する場合)。</p> <p>シスコでは、ソフトウェアに通知ビューを自動生成させることを推奨しています。このドキュメントの「通知ビューの設定」の項を参照してください。</p>
access	<p>(任意) グループに関連付ける標準アクセスコントロールリスト (ACL) を指定します。</p>
ipv6	<p>(任意) IPv6 名前付きアクセスリストを指定します。IPv6 と IPv4 の両方のアクセスリストが示されている場合は、IPv6 名前付きアクセスリストがリストの最初に表示されている必要があります。</p>
<i>named-access-list</i>	<p>(任意) IPv6 アクセスリストの名前。</p>
<i>acl-number</i>	<p>(任意) <i>acl-number</i> 引数は、以前に設定された標準アクセスリストを識別する 1 ~ 99 の整数です。</p>
<i>acl-name</i>	<p>(任意) <i>acl-name</i> 引数は、以前に設定された標準アクセスリストの名前である最大 64 文字の文字列です。</p>

Command Default SNMP サーバグループは設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.8.1a	このコマンドが導入されました。

Usage Guidelines

コミュニティストリングが内部的に設定されている場合、**public** という名前の 2 つのグループが自動生成されます。1 つは v1 セキュリティ モデル用、もう 1 つは v2c セキュリティ モデル用です。同様に、コミュニティストリングを削除すると、**public** という名前の v1 グループと **public** という名前の v2c グループが削除されます。

snmp-server group コマンドを設定する際、認証やプライバシーアルゴリズムにはデフォルト値はありません。また、デフォルトのパスワードも存在しません。Message Digest 5 (MD5) パスワードの指定については、**snmp-server user** コマンドのドキュメントを参照してください。

通知ビューの設定

notify view オプションは、2 つの目的に使用できます。

- グループに SNMP を使用して設定された通知ビューがあり、その通知ビューを変更する必要がある。
- **snmp-server host** コマンドは、**snmp-server group** コマンドの前に設定されている可能性があります。この場合、**snmp-server host** コマンドを再設定するか、または適切な通知ビューを指定する必要があります。

次の理由から、SNMP グループを設定する際に通知ビューを指定することは推奨されていません。

- **snmp-server host** コマンドによってユーザに対して自動生成された通知ビューを、そのユーザに関連付けられているグループに追加する。
- グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。

snmp-server group コマンドの一部としてグループの通知ビューを指定する代わりに、指定された順序で次のコマンドを使用します。

1. **snmp-server user:** SNMP ユーザを設定します。
2. **snmp-server group:** 通知ビューを追加しないで SNMP グループを設定します。
3. **snmp-server host:** トラップ操作の受信者を指定して、通知ビューを自動生成します。

SNMP コンテキスト

SNMP コンテキストによって、MIB データにアクセスする安全な方法が VPN ユーザに提供されます。VPN がコンテキストに関連付けられると、VPN 固有の MIB データがそのコンテキストに存在します。VPN をコンテキストに関連付けると、サービス プロバイダーが、複数 VPN でネットワークを管理できます。コンテキストを作成して VPN に関連付けることにより、サービス プロバイダーは、ある VPN のユーザが同じネットワークング デバイス上で他の VPN のユーザに関する情報にアクセスするのを防ぐことができます。

読み取り、書き込み、または通知 SNMP ビューを SNMP コンテキストに関連付けるには、**context context-name** キーワードおよび引数とともにこのコマンドを使用します。

SNMP グループの作成

次の例は、SNMP サーバグループ「public」を作成して、すべてのオブジェクトに対して標準名前付きアクセスリスト「lmnop」のメンバへの読み取り専用アクセスを許可する方法を示しています。

```
Device(config)# snmp-server group public v2c access lmnop
```

SNMP サーバグループの削除

次の例に、設定から SNMP サーバグループ「public」を削除する方法を示します。

```
Device(config)# no snmp-server group public v2c
```

SNMP サバグループと指定されたビューとの関連付け

次の例に、SNMPv2c グループ「GROUP1」のビューに関連付けられた SNMP コンテキスト「A」を示します。

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	デバイス上のグループの名前、セキュリティモデル、各種ビューのステータス、および各グループのストレージタイプを表示します。
snmp mib community-map	SNMP コミュニティを SNMP コンテキスト、エンジン ID、セキュリティ名、または VPN ターゲットリストに関連付けます。
snmp-server host	SNMP 通知動作の受信者を指定します。
snmp-server user	SNMP グループに新しいユーザを設定します。

snmp-server host

Simple Network Management Protocol (SNMP) 通知操作の受信者 (ホスト) を指定するには、デバイスで **snmp-server host** グローバル コンフィギュレーション コマンドを使用します。指定したホストを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server host {host-addr} [vrf vrf-instance] [informs | traps] [version {1 | 2c | 3
{auth | noauth | priv} } ] {community-string [notification-type] }
no snmp-server host {host-addr} [vrf vrf-instance] [informs | traps] [version {1 | 2c | 3
{auth | noauth | priv} } ] {community-string [notification-type] }
```

Syntax Description

<i>host-addr</i>	ホスト (ターゲットとなる受信側) の名前またはインターネットアドレスです。
vrf <i>vrf-instance</i>	(任意) 仮想プライベート ネットワーク (VPN) ルーティング インスタンスとこのホストの名前を指定します。
informs traps	(任意) このホストに SNMP トラップまたは情報を送信します。
version 1 2c 3	(任意) トラップの送信に使用する SNMP のバージョンを指定します。 1 : SNMPv1。情報の場合は、このオプションを使用できません。 2c : SNMPv2C。 3 : SNMPv3。認証キーワードの1つ (次の表の行を参照) が、バージョン3キーワードに従っている必要があります。
auth noauth priv	auth (任意): Message Digest 5 (MD5) およびセキュア ハッシュ アルゴリズム (SHA) パケット 認証をイネーブルにします。 noauth (デフォルト): noAuthNoPriv セキュリティ レベル。 auth noauth priv キーワードの選択が指定されていない場合、これがデフォルトとなります。 priv (任意): データ暗号規格 (DES) によるパケット暗号化 (「プライバシー」ともいう) をイネーブルにします。
<i>community-string</i>	通知処理にともなって送信される、パスワードと類似したコミュニティ ストリングです。 snmp-server host コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、 snmp-server community グローバル コンフィギュレーション コマンドを使用してから、 snmp-server host コマンドを使用することを推奨します。
Note	コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。

notification-type (任意) ホストに送信される通知のタイプです。タイプが指定されていない場合、すべての通知が送信されます。通知タイプには、次のキーワードの1つまたは複数指定できます。

- **auth-framework:** SNMP CISCO-AUTH-FRAMEWORK-MIB トラップを送信します。
 - **bridge:** SNMP スパニング ツリー プロトコル (STP) ブリッジ MIB トラップを送信します。
 - **bulkstat:** データ収集 MIB 収集通知トラップを送信します。
 - **call-home:** SNMP CISCO-CALLHOME-MIB トラップを送信します。
 - **cef:** SNMP CEF トラップを送信します。
 - **config:** SNMP 設定トラップを送信します。
 - **config-copy:** SNMP config-copy トラップを送信します。
 - **config-ctid:** SNMP config-ctid トラップを送信します。
 - **copy-config:** SNMP コピー設定トラップを送信します。
 - **cpu:** CPU 通知トラップを送信します。
 - **cpu threshold:** CPU しきい値通知トラップを送信します。
 - **entity:** SNMP エントリ トラップを送信します。
-

- **envmon:** 環境モニタ トラップを送信します。
- **errdisable:** SNMP errdisable 通知トラップを送信します。
- **event-manager:** SNMP Embedded Event Manager トラップを送信します。
- **flash:** SNMP FLASH 通知を送信します。
- **flowmon:** SNMP flowmon 通知トラップを送信します。
- **ipmulticast:** SNMP IP マルチキャストルーティングトラップを送信します。
- **ipsla:** SNMP IP SLA トラップを送信します。
- **license:** ライセンス トラップを送信します。
- **local-auth:** SNMP ローカル認証トラップを送信します。
- **mac-notification:** SNMP MAC 通知トラップを送信します。
- **pim:** SNMP プロトコル独立型マルチキャスト (PIM) トラップを送信します。
- **power-ethernet:** SNMP パワーイーサネット トラップを送信します。
- **snmp:** SNMP タイプ トラップを送信します。
- **storm-control:** SNMP ストーム制御トラップを送信します。
- **stp:** SNMP STP 拡張 MIB トラップを送信します。
- **syslog:** SNMP syslog トラップを送信します。
- **transceiver:** SNMP トランシーバ トラップを送信します。
- **tty:** TCP 接続トラップを送信します。
- **vlan-membership:** SNMP VLAN メンバーシップ トラップを送信します。
- **vlancreate:** SNMP VLAN 作成のトラップを送信します。
- **vlandelete:** SNMP VLAN 削除トラップを送信します。
- **vrfmib:** SNMP vrfmib トラップを送信します。
- **vtp:** SNMP VLAN Trunking Protocol (VTP) トラップを送信します。
- **wireless:** ワイヤレス トラップを送信します。

Command Default

このコマンドは、デフォルトでディセーブルになっています。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップタイプがホストに送信されます。情報はこのホストに送信されません。

version キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで **noauth** (noAuthNoPriv) セキュリティレベルになります。



Note **fru-ctrl** キーワードは、コマンドラインのヘルプストリングには表示されますが、サポートされていません。

Command Modes グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

SNMP 通知は、トラップまたは情報要求として送信できます。トラップを受信しても受信側は確認応答を送信しないため、トラップは信頼できません。送信側では、トラップを受信されたかどうかを判別できません。ただし、情報要求を受信した SNMP エンティティは、SNMP 応答 PDU を使用してメッセージに確認応答します。送信側が応答を受信しない場合、インフォーム要求を再送信して、インフォームが目的の宛先に到達する可能性を向上できます。

ただし、情報はエージェントおよびネットワークのリソースをより多く消費します。送信と同時に破棄されるトラップと異なり、インフォーム要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。また、トラップの送信は 1 回限りですが、情報は数回にわたって再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

snmp-server host コマンドを入力しなかった場合は、通知が送信されません。SNMP 通知を送信するようにデバイスを設定するには、**snmp-server host** コマンドを少なくとも 1 つ入力する必要があります。キーワードを指定しないでこのコマンドを入力した場合、そのホストではすべてのトラップタイプがイネーブルになります。複数のホストをイネーブルにするには、ホストごとに **snmp-server host** コマンドを個別に入力する必要があります。コマンドには複数の通知タイプをホストごとに指定できます。

ローカルユーザがリモートホストと関連付けられていない場合、デバイスは **auth** (authNoPriv) および **priv** (authPriv) の認証レベルの情報を送信しません。

同じホストおよび同じ種類の通知（トラップまたは情報）に対して複数の **snmp-server host** コマンドを指定した場合は、後に入力されたコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドだけが有効です。たとえば、ホストに **snmp-server host inform** コマンドを入力してから、同じホストに別の **snmp-server host inform** コマンドを入力した場合は、2 番目のコマンドによって最初のコマンドが置き換えられます。

snmp-server host コマンドは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと組み合わせて使用します。グローバルに送信される SNMP 通知を指定するには、**snmp-server enable traps** コマンドを使用します。1 つのホストでほとんどの通知を受信する場合は、このホストに対して、少なくとも 1 つの **snmp-server enable traps** コマンドと **snmp-server host** コマンドをイネーブルにする必要があります。一部の通知タイプは、**snmp-server enable traps** コマンドで制

御できません。たとえば、ある通知タイプは常にイネーブルですが、別の通知タイプはそれぞれ異なるコマンドによってイネーブルになります。

キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** コマンドを使用してください。

Examples

次の例では、トラップに対して一意の SNMP コミュニティ スtring **comaccess** を設定し、この String による、アクセス リスト **10** を介した SNMP ポーリング アクセスを禁止します。

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(config)# access-list 10 deny any
```

次の例では、名前 **myhost.cisco.com** で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ String は、**comaccess** として定義されています。

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティ String **public** を使用して、すべてのトラップをホスト **myhost.cisco.com** に送信するようにデバイスをイネーブルにする方法を示します。

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

snmp-server manager

Simple Network Management Protocol (SNMP) マネージャプロセスを起動するには、グローバル コンフィギュレーション モードで **snmp-server manager** コマンドを使用します。SNMP マネージャ プロセスを停止するには、このコマンドの **no** 形式を使用します。

snmp-server manager
no snmp-server manager

Command Default

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Usage Guidelines

SNMP マネージャプロセスは SNMP 要求をエージェントに送信し、エージェントから SNMP 応答と通知を受け取ります。SNMP マネージャプロセスがイネーブルになっているときには、ルータはその他の SNMP エージェントに問い合わせ、送信されてきた SNMP トラップを処理できません。

ほとんどのネットワークセキュリティポリシーでは、ルータが SNMP 要求を受け付け、SNMP 応答を送信し、SNMP 通知を送信するものと想定されています。SNMP マネージャ機能がイネーブルになっている状態では、ルータは、SNMP 要求の送信、SNMP 応答の受信、および SNMP 通知の受信も行います。場合によっては、この機能をイネーブルにする前にセキュリティポリシーの実装を更新する必要がある場合もあります。

通常、SNMP 要求は UDP ポート 161 に送信されます。通常、SNMP 応答は UDP ポート 161 から送信されます。通常、SNMP 通知は UDP ポート 162 に送信されます。

次に、SNMP マネージャプロセスをイネーブルにする例を示します。

```
Router(config)# snmp-server manager
```

Related Commands

Command	Description
show running-config	現在実行中のコンフィギュレーション ファイルまたは特定のインターフェイスのコンフィギュレーションの内容、またはマップクラス情報を表示します。
show snmp user	グループユーザ名テーブルの各 SNMP ユーザ名に関する情報を表示します。
snmp-server engineID	デバイスで設定されたローカル SNMP エンジンおよびすべてのリモートエンジンの ID を表示します。

snmp-server user

Simple Network Management Protocol (SNMP) グループに新しいユーザを設定するには、グローバル コンフィギュレーション モードで **snmp-server user** コマンドを使用します。SNMP グループからユーザを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server user username group-name [remote host [udp-port port] [vrf vrf-name ]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access [ipv6 nacl] [priv {des | 3des | aes {128 | 192 | 256}} privpassword] {acl-numberacl-name}]
no snmp-server user username group-name [remote host [udp-port port] [vrf vrf-name ]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access [ipv6 nacl] [priv {des | 3des | aes {128 | 192 | 256}} privpassword] {acl-numberacl-name}]
```

Syntax Description

<i>username</i>	エージェントに接続する、ホスト上のユーザの名前。
<i>group-name</i>	エントリが属する ACL (アクセス コントロール リスト) 名
remote	(任意) ユーザが属するリモート SNMP エンティティ、およびそのエンティティのホスト名または IPv6 アドレスまたは IPv4 IP アドレスを指定します。IPv6 アドレスおよび IPv4 IP アドレスの両方を指定すると、IPv6 ホストが最初に表示されます。
<i>host</i>	(任意) リモート SNMP ホストの名前または IP アドレス。
udp-port	(任意) リモート ホストのユーザ データグラム プロトコル (UDP) ポート番号を指定します。
<i>port</i>	(任意) UDP ポートを識別する整数値。デフォルトは 162 です。
vrf	(任意) ルーティング テーブルのインスタンスを指定します。
<i>vrf-name</i>	(任意) データの格納に使用するバーチャルプライベートネットワーク (VPN) ルーティングおよび転送 (VRF) テーブルの名前。
v1	SNMPv1 を使用することを指定します。
v2c	SNMPv2c を使用することを指定します。
v3	SNMPv3 セキュリティ モデルを使用することを指定します。 encrypted キーワードまたは auth キーワード、あるいはその両方の使用を許可します。
encrypted	(任意) パスワードが暗号化された形式で表示されるかどうかを指定します。
auth	(任意) 使用する認証レベルを指定します。
md5	(任意) HMAC-MD5-96 認証レベルを指定します。
sha	(任意) HMAC-SHA-96 認証レベルを指定します。

<i>auth-password</i>	(任意) エージェントがホストからパケットを受信できるようにするストリング (64 文字以下)。
access	(任意) この SNMP ユーザと関連付けるアクセス コントロール リスト (ACL) を指定します。
ipv6	(任意) この SNMP ユーザと関連付ける IPv6 名前付きアクセス リストを指定します。
<i>nacl</i>	(任意) ACL の名前です。IPv4、IPv6、または IPv4 と IPv6 の両方のアクセス リストを指定できます。両方を指定した場合は、IPv6 名前付きアクセス リストがステートメントの最初に表示されます。
priv	(任意) SNMP メッセージ レベルの安全性のための SNMP バージョン 3 のユーザベースセキュリティ モデル (USM) の使用を指定します。
des	(任意) 暗号化について 56 ビット Digital Encryption Standard (DES) アルゴリズムの使用を指定します。
3des	(任意) 暗号化について 168 ビット 3DES アルゴリズムの使用を指定します。
aes	(任意) 暗号化について Advanced Encryption Standard (AES) アルゴリズムの使用を指定します。
128	(任意) 暗号化について 128 ビット AES アルゴリズムの使用を指定します。
192	(任意) 暗号化について 192 ビット AES アルゴリズムの使用を指定します。
256	(任意) 暗号化について 256 ビット AES アルゴリズムの使用を指定します。
<i>privpassword</i>	(任意) プライバシー ユーザ パスワードを指定する文字列 (64 文字以下)。
<i>acl-number</i>	(任意) IP アドレスの標準アクセス リストを指定する 1 ~ 99 の範囲の整数。
<i>acl-name</i>	(任意) IP アドレスの標準アクセス リストの名前である文字列 (64 文字以下)。

Command Default

暗号化、パスワード、およびアクセス リストのデフォルト動作については、「[使用上のガイドライン](#)」の項にある表を参照してください。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.8.1a	このコマンドが導入されました。

Usage Guidelines

リモートユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。また、特定のエージェントにリモートユーザを設定する前に、**snmp-server engineID** コマンドに **remote** キーワードを指定して SNMP エンジン

ンIDを設定します。リモートエージェントのSNMPエンジンIDは、パスワードから認証とプライバシーダイジェストを計算する際に必要です。最初にリモートエンジンIDが設定されていない場合、コンフィギュレーションコマンドは失敗します。

privpassword 引数と *auth-password* 引数については、最小の長さが1文字で、推奨される長さは8文字以上であり、文字と数字の両方を含める必要があります。推奨される最大長は64文字です。次の表に、暗号化、パスワード、およびアクセスリストのデフォルトのユーザ特性を示します。

Table 112: *snmp-server user* のデフォルトの説明

特性	デフォルト
アクセスリスト	すべてのIPアクセスリストからのアクセスが許可されます。
暗号化	デフォルトでは存在しません。 encrypted キーワードは、パスワードがメッセージダイジェストアルゴリズム5 (MD5) ダイジェストであり、テキストパスワードではないことを指定するために使用されます。
パスワード	テキスト文字列と見なされます。
リモートユーザ	すべてのユーザは、 remote キーワードを使用してリモートであることを指定しないかぎり、このSNMPエンジンに対してローカルであると見なされます。

SNMPパスワードは、権威SNMPエンジンのSNMPIDを使用してローカライズされます。インフォームの場合、正規のSNMPエージェントはリモートエンジンです。プロキシ要求またはインフォームを送信できるようにするには、SNMPデータベース内のリモートエンジンのSNMPエンジンIDを設定する必要があります。



Note SNMPユーザ設定後にエンジンIDを変更すると、ユーザを削除できません。ユーザを削除するには、まず、SNMPユーザを再設定する必要があります。

パスワードおよびダイジェストの取り扱い

コマンドを設定する際、認証やプライバシーアルゴリズムにはデフォルト値はありません。また、デフォルトのパスワードも存在しません。パスワードの最小の長さは1文字ですが、シスコではセキュリティのために8文字以上を推奨しています。パスワードの推奨される最大長は64文字です。パスワードを忘れた場合は回復できないため、ユーザを再設定する必要があります。プレーンテキストのパスワードとローカライズされたMD5ダイジェストの、どちらも指定できます。

ローカライズされたMD5またはセキュアハッシュアルゴリズム(SHA)ダイジェストを持っている場合は、プレーンテキストのパスワードではなく、その文字列を指定できます。ダイジェストはaa:bb:cc:ddの形式にする必要があります。aa、bb、およびccは16進値です。また、ダイジェストは正確に16個のオクテットであることが必要です。

Examples

次の例は、ユーザ `abcd` を `public` という名前の SNMP サーバグループに追加する方法を示しています。この例では、ユーザにアクセスリストが指定されていないため、グループに適用されている標準の名前付きアクセスリストがユーザに適用されます。

```
Device(config)# snmp-server user abcd public v2c
```

次の例は、ユーザ `abcd` を `public` という名前の SNMP サーバグループに追加する方法を示しています。この例では、標準の名前付きアクセスリスト `qrst` からのアクセスルールがユーザに適用されます。

```
Device(config)# snmp-server user abcd public v2c access qrst
```

次の例では、プレーンテキストのパスワード `cisco123` が、`public` という名前の SNMP サーバグループのユーザ `abcd` に対して設定されています。

```
Device(config)# snmp-server user abcd public v3 auth md5 cisco123
```

`show running-config` コマンドを入力すると、このユーザの行が表示されます。このユーザが設定に追加されたことを確認するには、`show snmp user` コマンドを使用します。



Note `show running-config` コマンドは、`noAuthNoPriv` モードで作成されたユーザを表示しますが、`authPriv` モードまたは `authNoPriv` モードで作成されたアクティブな SNMP ユーザは表示しません。`authPriv`、`authNoPriv`、または `noAuthNoPriv` モードで作成したアクティブな SNMPv3 ユーザを表示するには、`show snmp user` コマンドを使用します。

ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーンテキストのパスワードではなく、その文字列を指定できます。ダイジェストは `aa:bb:cc:dd` の形式にする必要があります。`aa`、`bb`、および `cc` は 16 進値です。また、ダイジェストは正確に 16 個のオクテットであることが必要です。

次の例では、プレーンテキストのパスワードの代わりに MD5 ダイジェスト文字列が使用されています。

```
Device(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

次の例では、ユーザ `abcd` が `public` という名前の SNMP サーバグループから削除されます。

```
Device(config)# no snmp-server user abcd public v2c
```

次の例では、`public` という名前の SNMP サーバグループからのユーザ `abcd` が、`secure3des` をパスワードとして使用してプライバシーの暗号化のために 168 ビット 3DES アルゴリズムを使用することを指定しています。

```
Device(config)# snmp-server user abcd public priv v2c 3des secure3des
```

Related Commands	Command	Description
	show running-config	現在実行中のコンフィギュレーションファイルまたは特定のインターフェイスのコンフィギュレーションの内容、またはマップクラス情報を表示します。
	show snmp user	グループユーザ名テーブルの各 SNMP ユーザ名に関する情報を表示します。
	snmp-server engineID	デバイスで設定されたローカル SNMP エンジンおよびすべてのリモートエンジンの ID を表示します。

snmp-server view

ビューエントリを作成または更新するには、グローバル コンフィギュレーション モードで **snmp-server view** コマンドを使用します。指定された Simple Network Management Protocol (SNMP) サーバビューエントリを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server view view-name oid-tree {included | excluded}
no snmp-server view view-name
```

Syntax Description

view-name	更新または作成しているビュー レコードのラベル。レコードはこの名前で参照されます。
oid-tree	ビューに含める、またはビューから除外する ASN.1 サブツリーのオブジェクト識別子。サブツリーを識別するために、1.3.6.2.4 などの数字や system などの単語で構成されるテキスト文字列を指定します。サブツリーファミリを指定するには、サブIDの1文字をアスタリスク (*) ワイルドカードに変えます。たとえば、1.3.*.4 です。
included	oid-tree 引数に指定されている OID (およびサブツリーOID) を SNMP ビューに含めるように設定します。
excluded	oid-tree 引数に指定されている OID (およびサブツリーOID) を SNMP ビューから明示的に除外するように設定します。

Command Default

ビュー エントリは存在しません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.8.1a	このコマンドが導入されました。

Usage Guidelines

他の SNMP コマンドでは、引数として **SMP** ビューが必要です。このコマンドを使用して、他のコマンドの引数として使用するビューを作成します。

ビューを定義する代わりに、ビューが必要なときに2つの標準の定義済みビューを使用できます。1つは *everything* で、ユーザがすべてのオブジェクトを表示することができることを示します。もう1つは *restricted* で、ユーザが **system**、**snmpStats**、**snmpParties** の3つのグループを表示できることを示します。定義済みビューは、RFC 1447 で説明されています。

最初に入力する **snmp-server** コマンドは、ルーティングデバイス上で SNMP をイネーブルにします。

Examples

次に、MIB-II サブツリー内のすべてのオブジェクトを含むビューを作成する例を示します。

```
snmp-server view mib2 mib-2 included
```

次に、MIB-II システム グループのすべてのオブジェクトおよび Cisco エンタープライズ MIB のすべてのオブジェクトを含むビューを作成する例を示します。

```
snmp-server view root_view system included
snmp-server view root_view cisco included
```

次に、sysServices (System 7) と MIB-II インターフェイス グループ内のインターフェイス 1 のすべてのオブジェクトを除く、MIB-II システム グループのすべてのオブジェクトを含むビューを作成する例を示します。

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

次の例では、USM、VACM、およびコミュニティ MIB は、ルート親「internet」の下にある他のすべての MIB とともにビュー「test」に明示的に含まれています。

```
! -- include all MIBs under the parent tree "internet"
snmp-server view test internet included
! -- include snmpUsmMIB
snmp-server view test 1.3.6.1.6.3.15 included
! -- include snmpVacmMIB
snmp-server view test 1.3.6.1.6.3.16 included
! -- exclude snmpCommunityMIB
snmp-server view test 1.3.6.1.6.3.18 excluded
```

Related Commands

Command	Description
snmp-server community	SNMP プロトコルへのアクセスを許可するようにコミュニティアクセス スtring を設定します。
snmp-server manager	SNMP マネージャ プロセスを開始します。

source

Flexible NetFlow フローエクスポートから送信されるすべてのパケットの送信元 IP アドレスのインターフェイスを設定するには、フロー エクスポート コンフィギュレーション モードで **source** コマンドを使用します。Flexible NetFlow フローエクスポートから送信されるすべてのパケットの送信元 IP アドレスのインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
source interface-type interface-number
no source
```

Syntax Description	<i>interface-type</i>	Flexible NetFlow フローエクスポートから送信されるパケットの送信元 IP アドレス向けに使用する IP アドレスのインターフェイスのタイプ。
	<i>interface-number</i>	Flexible NetFlow フローエクスポートから送信されるパケットの送信元 IP アドレス向けに使用する IP アドレスのインターフェイス番号。
Command Default	Flexible NetFlow データグラムを送信するインターフェイスの IP アドレスが、送信元 IP アドレスとして使用されます。	
Command Modes	フロー エクスポート コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。	
Usage Guidelines	Flexible NetFlow が送信するデータグラムに一貫した送信元 IP アドレスを使用することの利点として、以下が含まれます。	

- Flexible NetFlow によりエクスポートされるデータグラムの送信元 IP アドレスは、Flexible NetFlow データがどちらのデバイスから到着するかを判断するために、宛先システムによって使用されます。デバイスから宛先システムに Flexible NetFlow データグラムを送信するのに使用できるパスがネットワークに複数あり、送信元 IP アドレスを取得する送信元インターフェイスが指定されていない場合、デバイスはデータグラムが送信されるインターフェイスの IP アドレスを、データグラムの送信元 IP アドレスとして使用します。この場合、宛先システムは同じデバイスから送信元 IP アドレスが異なる Flexible NetFlow データグラムを受信する場合があります。宛先システムが、異なる送信元 IP アドレスを持つ同じデバイスから Flexible NetFlow データグラムを受信すると、宛先システムは異なるデバイスから送信されたものとして Flexible NetFlow データグラムを処理します。宛先システムが Flexible NetFlow データグラムを異なるデバイスから送信されたものとして処理しないようにするには、宛先システムがデバイスですべての可能な送信元 IP アドレスから受信する Flexible NetFlow データグラムを単一の Flexible NetFlow フローに集約するように、宛先システムを設定する必要があります。
- データグラムを宛先システムに送信するために使用できる複数のインターフェイスがデバイスにあり、**source** コマンドを設定していない場合、Flexible NetFlow トラフィックを許可する

ために作成するアクセスリストに、各インターフェイスのIPアドレスのエントリを追加する必要があります。既知の送信元からのFlexible NetFlowトラフィックを許可し、不明な送信元からはブロックするためにアクセスリストを作成および維持することは、Flexible NetFlowトラフィックをエクスポートするデバイスごとに単一のIPアドレスにFlexible NetFlow データグラムの送信元IPアドレスを制限すると、より簡単に行えるようになります。



Caution **source** インターフェイスとして設定するインターフェイスには、設定されたIPアドレスが必須であり、アップされている必要があります。



Tip **source** コマンドで設定したインターフェイス上で一時的な停止が発生した場合、Flexible NetFlow エクスポートは、データグラムが送信されるインターフェイスのIPアドレスをデータグラムの送信元IPアドレスとして使用するデフォルトの動作に戻ります。この問題を回避するには、ループバックインターフェイスを送信元インターフェイスとして使用します。これは、ループバックインターフェイスが物理インターフェイスで発生する可能性のある一時的な停止の影響を受けないためです。

このコマンドをデフォルト設定に戻すには、**no source** または **default source** フロー エクスポート コンフィギュレーション コマンドを使用します。

Examples

次に、NetFlow トラフィックの送信元インターフェイスとして、ループバック インターフェイスを使用するように Flexible NetFlow を設定する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# source loopback 0
```

socket

クライアントソケットを指定し、TCL インタープリタの TCP over IPv4/IPv6 を経由した接続を可能にし、TCP ネットワーク接続を開くには、TCL で **socket** コマンドを使用します。

socket myaddr address myport port myvrf vrf-table-name host port

Syntax Description

myaddr	接続に必要なクライアント側ネットワーク インターフェイスのドメイン名または数値 IP アドレスを指定します。特にクライアントのマシンに複数のネットワーク インターフェイスがある場合はこのオプションを使用します。
myport	クライアントの接続に必要なポート番号を指定します。
myvrf	vrf テーブル名を指定します。vrf テーブルが設定されていない場合、コマンドは TCL_ERROR を返します。

Command Default

Command Modes

TCL コンフィギュレーション モード

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	myvrf キーワードが導入されました。

switchport mode access

トランキングなし、タグなしの単一VLANイーサネットインターフェイスとしてインターフェイスを設定するには、テンプレートコンフィギュレーションモードで **switchport mode access** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport mode access
no switchport mode access

Syntax Description	switchport mode access トランキングなし、タグなしの単一VLANイーサネットインターフェイスとして、インターフェイスを設定します。				
Command Default	アクセスポートは、1つのVLANのトラフィックだけを伝送できます。アクセスポートは、デフォルトで、VLAN 1のトラフィックを送受信します。				
Command Modes	テンプレートコンフィギュレーション				
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Fuji 16.9.2</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Examples

次に、単一VLANインターフェイスを設定する例を示します。

```
Device(config-template)# switchport mode access
```

switchport voice vlan

指定された VLAN からのすべての音声トラフィックを転送するように指定するには、テンプレート コンフィギュレーション モードで **switchport voice vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport voice vlan vlan_id
no switchport voice vlan
```

Syntax Description	switchport voice vlan <i>vlan_id</i> すべての音声トラフィックを指定された VLAN 経由で転送するように指定します。				
Command Default	1 ~ 4094 の値を指定できます。				
Command Modes	テンプレート コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Examples

次に、指定された VLAN からのすべての音声トラフィックを転送するように指定する例を示します。

```
Device(config-template)# switchport voice vlan 20
```

ttl

存続可能時間（TTL）を設定するには、フローエクスポート コンフィギュレーション モードで **ttl** コマンドを使用します。TTL 値を削除するには、このコマンドの **no** 形式を使用します。

```
ttl ttl
no ttl ttl
```

Syntax Description	<i>ttl</i> エクスポートされたデータグラムの存続可能時間（TTL）値。指定できる範囲は 1 ～ 255 です。デフォルトは 255 です。				
Command Default	フローエクスポートでは TTL 値 255 が使用されています。				
Command Modes	フローエクスポート コンフィギュレーション				
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Fuji 16.9.2</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	このコマンドをデフォルト設定に戻すには、 no ttl または default ttl フローエクスポート コンフィギュレーション コマンドを使用します。 次に、TTL 値 15 を指定する例を示します。 <pre>Device(config)# flow exporter FLOW-EXPORTER-1 Device(config-flow-exporter)# ttl 15</pre>				

transport

Flexible NetFlow のフローエクスポートのトランスポートプロトコルを設定するには、フローエクスポート コンフィギュレーション モードで **transport** コマンドを使用します。フローエクスポートのトランスポートプロトコルを削除するには、このコマンドの **no** 形式を使用します。

```
transport udp udp-port
no transport udp udp-port
```

Syntax Description	udp <i>udp-port</i> トランスポートプロトコルとして User Datagram Protocol (UDP; ユーザデータグラムプロトコル) を指定し、UDP ポート番号を指定します。				
Command Default	フローエクスポートでは、UDP をポート 9995 で使用します。				
Command Modes	フローエクスポート コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	このコマンドをデフォルト設定に戻すには、 no transport または default transport flow exporter コンフィギュレーション コマンドを使用します。				

次に、トランスポートプロトコルとして UDP を設定し、UDP ポート番号を 250 に設定する例を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# transport udp 250
```

template data timeout

フロー エクスポート テンプレート データの再送信のタイムアウト期間を指定するには、フロー エクスポート コンフィギュレーション モードで **template data timeout** コマンドを使用します。フロー エクスポートの再送信のタイムアウトを削除するには、このコマンドの **no** 形式を使用します。

template data timeout *seconds*
no template data timeout *seconds*

Syntax Description

seconds 秒単位のタイムアウト値です。指定できる範囲は 1 ~ 86400 です。デフォルトは 600 です。

Command Default

デフォルトのフロー エクスポート テンプレート再送信のタイムアウトは、600 秒です。

Command Modes

フロー エクスポート コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

フロー エクスポートのテンプレート データには、エクスポートされるデータ レコードが記述されています。対応するテンプレートなしでデータ レコードをデコードすることはできません。**template data timeout** コマンドを使用して、これらのテンプレートをエクスポートする頻度を制御します。

このコマンドをデフォルト設定に戻すには、**no template data timeout** または **default template data timeout** フロー レコード エクスポート コマンドを使用します。

次の例では、1000 秒というタイムアウトに基づいてテンプレートの再送信を設定します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# template data timeout 1000
```

udp peek

UDP ソケットへのピークを有効にするには、TCL コンフィギュレーション モードで **udp_peek** コマンドを使用します。

udp_peek *socket* **buffersize** *buffer-size*

Syntax Description

buffersize バッファサイズを指定します。

Command Default

Command Modes

TCL コンフィギュレーション モード

Command History

リリース	変更内容
------	------

Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。
-------------------------------	-----------------



PART **VIII**

QoS

- [QoS コマンド, on page 1131](#)



QoS コマンド

- [auto qos classify](#), on page 1132
- [auto qos trust](#), on page 1135
- [auto qos video](#), on page 1143
- [auto qos voip](#) , on page 1154
- [class](#), on page 1168
- [class-map](#), on page 1171
- [debug auto qos](#), on page 1173
- [match](#) (クラスマップ コンフィギュレーション) , on page 1174
- [policy-map](#), on page 1178
- [priority](#), on page 1181
- [qos queue-softmax-multiplier](#), on page 1183
- [queue-buffers ratio](#), on page 1184
- [queue-limit](#), on page 1185
- [random-detect cos](#), on page 1187
- [random-detect cos-based](#), on page 1189
- [random-detect dscp](#), on page 1190
- [random-detect dscp-based](#), on page 1192
- [random-detect precedence](#), on page 1193
- [random-detect precedence-based](#), on page 1195
- [service-policy](#) (有線) , on page 1196
- [set](#), on page 1198
- [show auto qos](#) , on page 1204
- [show class-map](#), on page 1206
- [show platform hardware fed switch](#), on page 1207
- [show platform software fed switch qos](#), on page 1211
- [show platform software fed switch qos qsb](#), on page 1212
- [show policy-map](#), on page 1215
- [show tech-support qos](#), on page 1217
- [trust device](#), on page 1219

auto qos classify

QoS ドメイン内で信頼できないデバイスの Quality of Service (QoS) の分類を自動的に設定するには、インターフェイスコンフィギュレーションモードで **auto qos classify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos classify [police]
no auto qos classify [police]

Syntax Description	police (任意) 信頼できないデバイスの QoS ポリシングを設定します。
---------------------------	---

Command Default	auto-QoS 分類は、すべてのポートでディセーブルです。
------------------------	--------------------------------

Command Modes	インターフェイス コンフィギュレーション
----------------------	----------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、デバイス、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジデバイスなどが含まれます。

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。

auto-QoS は、デバイスが信頼インターフェイスと接続するように設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッドポートの場合は、着信パケットの CoS 値が信頼されません。ルーテッドポートでは、着信パケットの DSCP 値が信頼されます。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。



Note デバイスは、コマンドラインインターフェイス (CLI) からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。 **debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッグがイネーブルになります。

auto qos classify コマンドおよび **auto qos classify police** コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ (**auto qos classify police** コマンドの場合) :

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ:

- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

ポートの auto-QoS をディセーブルにするには、**no auto qos classify** インターフェイス コンフィギュレーションコマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイスコンフィギュレーションコマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos classify** コマンドを入力すると、auto-QoS によって生成されたグローバルコンフィギュレーションコマンドが残っている場合でも、auto-QoS はディセーブルと見なされ

ます（グローバルコンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

Examples

次の例では、信頼できないデバイスの auto-QoS 分類をイネーブルにし、トラフィックをポリシングする方法を示します。

設定を確認するには、**show auto qos interface *interface-id*** 特権 EXEC コマンドを入力します。

auto qos trust

QoS ドメイン内の信頼インターフェイスの Quality of Service (QoS) を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
auto qos trust {cos|dscp}
no auto qos trust {cos|dscp}
```

Syntax Description

cos CoS パケット分類を信頼します。

dscp DSCP パケット分類を信頼します。

Command Default

auto-QoS 信頼は、すべてのポートでディセーブルです。

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、デバイス、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジデバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。

Table 113: トラフィックタイプ、パケットラベル、およびキュー

	VoIP データ トラフィック	VOIP コン トロール トラ フィック	ルーティン グプロト コルトラ フィック	STP ² BPDU ³ ト ラフィック	リアルタイム ビデオ トラフィッ ク	その他すべてのト ラフィック
DSCP ⁴	46	24、26	48	56	34	–
CoS ⁵	5	3	6	7	3	–

² STP = スパニング ツリー プロトコル

³ BPDU = ブリッジプロトコルデータ ユニット

⁴ DSCP = DiffServ コードポイント

⁵ CoS = サービスクラス



Note デバイスは、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。 **debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッグがイネーブルになります。

auto qos trust cos コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

auto qos trust dscp コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

ポートの auto-QoS をディセーブルにするには、**no auto qos trust** インターフェイス コンフィギュレーションコマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイスコンフィギュレーションコマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos trust** コマンドを入力すると、auto-QoS によって生成されたグローバルコンフィギュレーションコマンドが残っている場合でも、auto-QoS はディセーブルと見なされず（グローバルコンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

Examples

次に、特定の CoS 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
Device(config)# interface gigabitethernet1/0/17
Device(config-if)# auto qos trust cos
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/17

Gigabitethernet1/0/17

Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1
```

```

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
 0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
 0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 3
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

```

```
Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

次に、特定の DSCP 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
Device(config)# interface gigabitethernet1/0/18
Device(config-if)# auto qos trust dscp
Device(config-if)# end
Device#show policy-map interface gigabitethernet1/0/18
Gigabitethernet1/0/18
```

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

```
Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp dscp table AutoQos-4.0-Trust-Dscp-Table
```

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:

```
Queueing
  priority level 1
```

```
(total drops) 0
(bytes output) 0
```

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)

```
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,
```

```
  Priority Level: 1
```

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)

```
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
```

```
Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100
```

```
(total drops) 0
(bytes output) 0
bandwidth remaining 10%
```

```
queue-buffers ratio 10
```

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)

```
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
```

```
Queueing
```

```
(total drops) 0
(bytes output) 0
bandwidth remaining 10%
```

```
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
 Match: dscp af21 (18) af22 (20) af23 (22)
   0 packets, 0 bytes
   5 minute rate 0 bps
 Match: cos 2
   0 packets, 0 bytes
   5 minute rate 0 bps
 Queueing

 (total drops) 0
 (bytes output) 0
 bandwidth remaining 10%
 queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
 Match: dscp af11 (10) af12 (12) af13 (14)
   0 packets, 0 bytes
   5 minute rate 0 bps
 Match: cos 1
   0 packets, 0 bytes
   5 minute rate 0 bps
 Queueing

 (total drops) 0
 (bytes output) 0
 bandwidth remaining 4%
 queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
 Match: dscp cs1 (8)
   0 packets, 0 bytes
   5 minute rate 0 bps
 Queueing

 (total drops) 0
 (bytes output) 0
 bandwidth remaining 1%
 queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
 Match: dscp af31 (26) af32 (28) af33 (30)
   0 packets, 0 bytes
   5 minute rate 0 bps
 Queueing

 (total drops) 0
 (bytes output) 0
 bandwidth remaining 10%
 queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
 Match: any
   0 packets, 0 bytes
   5 minute rate 0 bps
 Queueing

 (total drops) 0
```

```
(bytes output) 0  
bandwidth remaining 25%  
queue-buffers ratio 25
```

設定を確認するには、**show auto qos interface *interface-id*** 特権 EXEC コマンドを入力します。

auto qos video

QoS ドメイン内のビデオの Quality Of Service (QoS) を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos video** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
auto qos video { cts | ip-camera | media-player }
no auto qos video { cts | ip-camera | media-player }
```

Syntax Description	cts	ip-camera	media-player
	Cisco TelePresence System に接続されるポートを指定し、自動的にビデオの QoS を設定します。	Cisco IP カメラに接続されるポートを指定し、自動的にビデオの QoS を設定します。	Cisco Digital Media Player に接続されるポートを指定し、自動的にビデオの QoS を設定します。

Command Default Auto-QoS ビデオは、ポート上でディセーブルに設定されています。

Command Modes インターフェイス コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines QoS ドメイン内のビデオトラフィックに適切な QoS を設定するには、このコマンドを使用します。QoS ドメインには、デバイス、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジデバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。詳細については、この項の最後にあるキューテーブルを参照してください。

auto-QoS は、Cisco TelePresence システム、Cisco IP カメラ、または Cisco Digital Media Player へのビデオ接続用にデバイスを設定します。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。

デバイスは、コマンドライン インターフェイス (CLI) からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、

デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが **auto-QoS** をイネーブルにする最初のポートの場合は、**auto-QoS** によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで **auto-QoS** をイネーブルにすると、そのポートに対して **auto-QoS** によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

auto-QoS をイネーブルにした後、名前に **AutoQoS** を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、**auto-QoS** をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、**auto-QoS** のデバッグがイネーブルになります。

auto qos video cts コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

auto qos video ip-camera コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

auto qos video media-player コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

ポートの auto-QoS をディセーブルにするには、**no auto qos video** インターフェイス コンフィギュレーションコマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーションコマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos video** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーションコマンドが残っている場合でも、auto-QoS はディセーブルと見なされます (グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため)。

Table 114: トラフィックタイプ、パケットラベル、およびキュー

	VoIP データ トラフィック	VOIP コントロール トラフィック	ルーティン グプロトコ ルトラフィッ ク	STP ⁶ BPD ⁷ U トラフィック	リアルタイム ビデオトラ フィック	その他すべての トラフィック
DSCP ⁸	46	24、26	48	56	34	—
CoS ⁹	5	3	6	7	3	—

⁶ STP = スパニング ツリー プロトコル

⁷ BPD⁷U = ブリッジ プロトコル データ ユニット

⁸ DSCP = DiffServ コードポイント

⁹ CoS = サービスクラス

Examples

次に、**auto qos video cts** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
Device(config)# interface gigabitethernet1/0/12
Device(config-if)# auto qos video cts
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/12
Gigabitethernet1/0/12

Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,
```

```
Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
```

```

    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25

```

次に、**auto qos video ip-camera** コマンドと、適用されるポリシーとクラスマップの例を示します。

```

Device(config)# interface gigabitethernet1/0/9
Device(config-if)# auto qos video ip-camera
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/9

```

Gigabitethernet1/0/9

```
Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy
```

```

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp dscp table AutoQos-4.0-Trust-Dscp-Table

```

```
Service-policy output: AutoQos-4.0-Output-Policy
```

```
queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
```

```

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25

```

次に、**auto qos video media-player** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
Device(config)# interface gigabitethernet1/0/7
```

```
Device(config-if)# auto qos video media-player
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/7

interface gigabitethernet1/0/7

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
```

```
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
```

```
Match: any
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

設定を確認するには、**show auto qos video interface *interface-id*** 特権 EXEC コマンドを入力します。

auto qos voip

QoS ドメイン内の Voice over IP (VoIP) の Quality of Service (QoS) を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos voip** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
auto qos voip {cisco-phone | cisco-softphone | trust}
no auto qos voip {cisco-phone | cisco-softphone | trust}
```

Syntax Description

cisco-phone	Cisco IP Phone に接続されるポートを指定し、自動的にビデオの VoIP を設定します。着信パケットの QoS ラベルが信頼されるのは、IP Phone が検知される場合に限ります。
cisco-softphone	Cisco SoftPhone が動作している装置に接続されるポートを指定し、自動的にビデオの VoIP を設定します。
trust	信頼できるデバイスに接続されるポートを指定し、自動的にビデオの VoIP を設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッドポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッドポートでは、着信パケットの DSCP 値が信頼されます。

Command Default

auto-QoS は、すべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。

Command Default

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

QoS ドメイン内の VoIP トラフィックに適切な QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、デバイス、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジデバイスなどが含まれます。

Auto-QoS は、デバイスとルーテッドポート上の Cisco IP 電話を使用した VoIP と、Cisco SoftPhone アプリケーションが動作する装置に対してデバイスを設定します。これらのリリースは Cisco IP SoftPhone バージョン 1.3(3)以降だけをサポートします。接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。



Note デバイスは、コマンドライン インターフェイス (CLI) からコマンドが入力された場合と同じように、**auto-QoS** によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、デバイスをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが **auto-QoS** をイネーブルにする最初のポートの場合は、**auto-QoS** によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで **auto-QoS** をイネーブルにすると、そのポートに対して **auto-QoS** によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

Cisco IP 電話に接続されたネットワークエッジのポートで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、デバイスにより信頼境界の機能が有効になります。デバイスは、Cisco Discovery Protocol (CDP) を使用して、Cisco IP 電話の存在を検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。また、デバイスはポリシングを使用してパケットがプロファイル内か、プロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、デバイスは DSCP 値を 0 に変更します。Cisco IP Phone が存在しない場合、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼しないように設定されます。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、デバイスが信頼境界の機能をイネーブルにします。

- Cisco SoftPhone が動作するデバイスに接続されたネットワークエッジにあるポートに **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合、デバイスはポリシングを使用してパケットがプロファイル内かプロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、デバイスは DSCP 値を 0 に変更します。
- ネットワーク内部に接続されたポート上で **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力すると、非ルーテッドポートの場合は入力パケット内の CoS 値、ルーテッドポートの場合は入力パケット内の DSCP 値がデバイスで信頼されます (前提条件は、トラフィックがすでに他のエッジデバイスによって分類されていることです)。

スタティックポート、ダイナミックアクセスポート、音声 VLAN アクセスポート、およびトランクポートで **auto-QoS** をイネーブルにすることができます。ルーテッドポートで Cisco IP Phone の自動 QoS を有効にすると、スタティック IP アドレスを IP Phone に割り当てます。



Note Cisco SoftPhone が稼働するデバイスがデバイスまたはルーテッドポートに接続されている場合、デバイスはポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。 **debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッグがイネーブルになります。

auto qos voip trust コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

auto qos voip cisco-softphone コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ:

- AutoQos-4.0-Voip-Data-Class (match-any)
- AutoQos-4.0-Voip-Signal-Class (match-any)
- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)

- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

auto qos voip cisco-phone コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ:

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
- service-policy output AutoQos-4.0-Output-Policy

クラスマップ:

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

ポートの auto-QoS をディセーブルにするには、**no auto qos voip** インターフェイス コンフィギュレーションコマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイスコンフィギュレーションコマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバルコンフィギュレーションコマンドが残っている場合でも、auto-QoS はディセーブルと見なされず（グローバルコンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

デバイスは、このテーブルの設定にしたがってポートの出力キューを設定します。

Table 115: 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS から キューへの マッピング	キュー ウェイト (帯域幅)	ギガビット対応 ポートのキュー (バッファ) サ イズ	10/100 イーサネッ トポートのキュー (バッファ) サイ ズ
プライオリティ (シェイプド)	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

Examples

次に、**auto qos voip trust** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
Device(config)# interface gigabitethernet1/0/31
Device(config-if)# auto qos voip trust
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/31
```

Gigabitethernet1/0/31

```
Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy
```

```
Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    cos cos table AutoQos-4.0-Trust-Cos-Table
```

```
Service-policy output: AutoQos-4.0-Output-Policy
```

```
queue stats for all priority classes:
```

```
Queueing
priority level 1
```

```
(total drops) 0
(bytes output) 0
```

```
Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
```

```
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,
```

```
Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
 0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 3
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 1
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
```

```

(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

次に、**auto qos voip cisco-phone** コマンドと、適用されるポリシーとクラスマップの例を示します。

```

Device(config)# interface gigabitethernet1/0/5
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/5

Gigabitethernet1/0/5

Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
 0 packets
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp ef
police:
  cir 128000 bps, bc 8000 bytes
  conformed 0 bytes; actions:

```

```
        transmit
    exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
        transmit
    exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
```

```

queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 1
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0

```

```

(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

次に、**auto qos voip cisco-softphone** コマンドと、適用されるポリシーとクラスマップの例を示します。

```

Device(config)# interface gigabitethernet1/0/20
Device(config-if)# auto qos voip cisco-softphone
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/20

Gigabitethernet1/0/20

Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
 0 packets
Match: dscp ef (46)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp ef
police:
  cir 128000 bps, bc 8000 bytes
 conformed 0 bytes; actions:
  transmit
 exceeded 0 bytes; actions:
  set-dscp-transmit dscp table policed-dscp
 conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
 0 packets
Match: dscp cs3 (24)
 0 packets, 0 bytes

```

```

    5 minute rate 0 bps
Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
QoS Set
    dscp cs3
police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
        transmit
    exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
    0 packets
Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
QoS Set
    dscp af41
police:
    cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
        transmit
    exceeded 0 bytes; actions:
        drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
    0 packets
Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
QoS Set
    dscp af11
police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
        transmit
    exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
    0 packets
Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
QoS Set
    dscp af21
police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
        transmit
    exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavenger-Class (match-any)
    0 packets
Match: access-group name AutoQos-4.0-Acl-Scavenger
    0 packets, 0 bytes
    5 minute rate 0 bps

```

```
QoS Set
  dscp cs1
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
Match: access-group name AutoQos-4.0-Acl-Signaling
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp cs3
police:
  cir 32000 bps, bc 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
Match: access-group name AutoQos-4.0-Acl-Default
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp default
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
  0 packets
Match: any
  0 packets, 0 bytes
  5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
  0 packets, 0 bytes
  5 minute rate 0 bps
Match: cos 5
  0 packets, 0 bytes
  5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,
```

```
Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
 0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 3
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 1
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
```

```
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

設定を確認するには、**show auto qos interface *interface-id*** 特権 EXEC コマンドを入力します。

class

指定されたクラスマップ名のトラフィックを分類する一致基準を定義するには、ポリシーマップ コンフィギュレーション モードで **class** コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

```
class {class-map-name | class-default}
no class {class-map-name | class-default}
```

Syntax Description

class-map-name クラスマップ名。

class-default 分類されていないパケットに一致するシステムのデフォルトクラスを参照します。

Command Default

ポリシーマップクラスマップは定義されていません。

Command Modes

ポリシー マップ コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

class コマンドを使用する前に、**policy-map** グローバル コンフィギュレーション コマンドを使用してポリシー マップを識別し、ポリシーマップ コンフィギュレーション モードを開始する必要があります。ポリシーマップを指定すると、ポリシーマップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシーマップをポートへ添付することができます。

class コマンドを入力すると、ポリシーマップ クラス コンフィギュレーション モードが開始されます。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **admit:** コールアドミッション制御 (CAC) の要求を許可します。
- **bandwidth:** クラスに割り当てられる帯域幅を指定します。
- **exit:** ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
- **no:** コマンドをデフォルト設定に戻します。
- **police:** 分類したトラフィックにポリサーまたは集約ポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。このコマンドの詳細については、Cisco.com で入手可能な『Cisco IOS Quality of Service Solutions Command Reference』を参照してください。

- **priority**: ポリシーマップに属するトラフィックのクラスにスケジューリングプライオリティを割り当てます。
- **queue-buffers**: クラスのキューバッファを設定します。
- **queue-limit**: ポリシーマップに設定されたクラスポリシー用にキューが保持できる最大パケット数を指定します。
- **service-policy**: QoS サービスポリシーを設定します。
- **set**: 分類したトラフィックに割り当てる値を指定します。詳細については、*set* コマンドを参照してください。
- **shape**: 平均またはピーク レート トラフィック シェーピングを指定します。このコマンドの詳細については、Cisco.com で入手可能な『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

class コマンドは、**class-map** グローバル コンフィギュレーション コマンドと同じ機能を実行します。他のポートと共有していない新しい分類が必要な場合は、**class** コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。

class class-default ポリシーマップ コンフィギュレーション コマンドを使用して、デフォルトクラスを設定できます。分類されていないトラフィック（トラフィッククラスで指定された一致基準を満たさないトラフィック）は、デフォルトトラフィックとして処理されます。

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

Examples

次に、**policy1** という名前のポリシー マップを作成する例を示します。入力方向に適用した場合、**class1** で定義されたすべての着信トラフィックのマッチングを行い、平均レート 1 Mb/s、バースト 1000 バイトでトラフィックをポリシングします。プロファイルを超えるトラフィックはテーブルマップでマークされます。

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police cir 1000000 bc 1000 conform-action
transmit exceed-action set-dscp-transmit dscp table EXEC_TABLE
Device(config-pmap-c)# exit
```

次に、ポリシー マップにデフォルトのトラフィッククラスを設定する例を示します。また、**class-default** が最初に設定された場合でも、デフォルトのトラフィッククラスをポリシーマップ **pm3** の終わりに自動的に配置する方法も示します。

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit
```

```
Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit
```

```
Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit
```

```
Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit
```

```
Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

class-map

名前を指定したクラスとパケットの照合に使用するクラスマップを作成し、クラスマップ コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **class-map** コマンドを使用します。既存のクラスマップを削除し、グローバルコンフィギュレーションモードまたはポリシー マップ コンフィギュレーションモードに戻るには、このコマンドの **no** 形式を使用します。

```
class-map class-map name {match-any | match-all}
no class-map class-map name {match-any | match-all}
```

Syntax Description

match-any	(任意) このクラスマップ内の一致ステートメントの論理和をとります。1 つ以上の条件が一致していなければなりません。
match-all	(任意) このクラスマップ内の一致ステートメントの論理積をとります。すべての条件に一致する必要があります。

class-map-name クラスマップ名。

Command Default

クラスマップは定義されていません。

Command Modes

グローバル コンフィギュレーション
ポリシー マップ コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

クラスマップ一致基準を作成または変更するクラスの名前を指定し、クラスマップコンフィギュレーションモードを開始する場合は、このコマンドを使用します。

ポートごとに適用される、グローバルに名前が付けられたサービスポリシーの一部として、パケットの分類、マーキング、および集約ポリシングを定義する場合は、**class-map** コマンドおよびそのサブコマンドを使用します。

Quality of Service (QoS) クラスマップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドを利用することができます。

- **description:** クラスマップを説明します (最大 200 文字)。 **show class-map** 特権 EXEC コマンドは、クラスマップの説明と名前を表示します。
- **exit:** QoS クラスマップ コンフィギュレーション モードを終了します。
- **match:** 分類基準を設定します。
- **no:** クラスマップから一致ステートメントを削除します。

match-any キーワードを入力した場合、**match access-group** クラスマップ コンフィギュレーション コマンドで名前付き拡張アクセスコントロールリスト (ACL) を指定するためにのみ使用できます。

物理ポート単位でパケット分類を定義するために、クラスマップごとに1つの **match** コマンドのみがサポートされています。

ACL には複数のアクセス コントロール エントリ (ACE) を含めることができます。



Note 同じクラスマップに IPv4 と IPv6 の分類基準を同時に設定することはできません。ただし、同じポリシー内の異なるクラスマップで設定することは可能です。

Examples

次に、クラスマップ `class1` に1つの一致基準 (アクセスリスト 103) を設定する例を示します。

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

次に、クラスマップ `class1` を削除する例を示します。

```
Device(config)# no class-map class1
```

設定を確認するには、**show class-map** 特権 EXEC コマンドを入力します。

debug auto qos

Automatic Quality of Service (auto-QoS; 自動 QoS) 機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug auto qos** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug auto qos
no debug auto qos

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

auto-QoS デバッグはディセーブルです。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。デバッグをイネーブルにするには、**debug auto qos** 特権 EXEC コマンドを入力します。

undebug auto qos コマンドは **no debug auto qos** コマンドと同じです。

あるデバイススタック上でデバッグをイネーブルにした場合、アクティブデバイスでのみイネーブルになります。スタックメンバのデバッグをイネーブルにする場合は、**session switch-number** 特権 EXEC コマンドでアクティブデバイスからセッションを開始してください。次に、スタックメンバのコマンドラインプロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバデバイスのデバッグをイネーブルにするには、アクティブデバイス上で **remote command stack-member-number LINE** 特権 EXEC コマンドを使用することもできます。

Examples

次の例では、auto-QoS がイネーブルの場合に自動的に生成される QoS 設定を表示する方法を示します。

```
Device# debug auto qos
AutoQoS debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# auto qos voip cisco-phone
```

match (クラスマップコンフィギュレーション)

トラフィックを分類するための一致基準を定義するには、クラスマップコンフィギュレーションモードで **match** コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

Cisco IOS XE Everest 16.5.x 以前のリリース

```
match {access-group {name acl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
no match {access-group {name acl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
```

Cisco IOS XE Everest 16.6.x 以降のリリース

```
match {access-group {name acl-name acl-index} | cos cos-value | dscp dscp-value | [ip] dscp dscp-list
| [ip] precedence ip-precedence-list | non-client-nrt | precedence precedence-value1...value4 | protocol
protocol-name | qos-group qos-group-value | vlan vlan-id | wlan wlan-id}
no match {access-group {name acl-name acl-index} | cos cos-value | dscp dscp-value | [ip] dscp
dscp-list | [ip] precedence ip-precedence-list | non-client-nrt | precedence precedence-value1...value4
| protocol protocol-name | qos-group qos-group-value | vlan vlan-id | wlan wlan-id}
```

Syntax Description

access-group	アクセスグループを指定します。
name <i>acl-name</i>	IP 標準または拡張アクセスコントロールリスト (ACL) または MAC ACL の名前を指定します。
<i>acl-index</i>	IP 標準または拡張アクセスコントロールリスト (ACL) または MAC ACL の番号を指定します。IP 標準 ACL の場合、ACL インデックス範囲は 1 ~ 99 および 1300 ~ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ~ 199 および 2000 ~ 2699 です。
class-map <i>class-map-name</i>	トラフィッククラスを分類ポリシーとして使用し、使用するトラフィッククラスの名前を一致基準として指定します。
cos <i>cos-value</i>	レイヤ 2 サービスクラス (CoS) /Inter-Switch Link (ISL) マーキングに基づいてパケットを照合します。CoS 値は 0 ~ 7 です。1 つの match cos ステートメントに最大 4 つの CoS 値をスペースで区切って指定できます。

dscp <i>dscp-value</i>	各 DSCP 値のパラメータを指定します。DiffServ コードポイント値を指定する 0 ~ 63 の範囲の値を指定できます。
ip dscp <i>dscp-list</i>	着信パケットとの照合を行うための、最大 8 つまでの IP DiffServ コードポイント (DSCP) 値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
ip precedence <i>ip-precedence-list</i>	着信パケットとの照合を行うための、最大 8 つの IP プレシデンス値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
precedence <i>precedence-value1...value4</i>	分類されたトラフィックに IP プレシデンス値を割り当てます。指定できる範囲は 0 ~ 7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
qos-group <i>qos-group-value</i>	特定の QoS グループ値を一致基準として識別します。指定できる範囲は 0 ~ 31 です。
vlan <i>vlan-id</i>	特定の VLAN を一致基準として指定します。指定できる範囲は 1 ~ 4094 です。
non-client-nrt	非クライアントの NRT (非リアルタイム) を照合します。
protocol <i>protocol-name</i>	プロトコルのタイプを指定します。
wlan <i>wlan-id</i>	802.11 特有の値を識別します。

Command Default

一致基準は定義されません。

Command Modes

クラスマップ コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入された。

Usage Guidelines

パケットを分類するために着信パケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。IP アクセス グループまたは MAC アクセス グループの Ether Type/Len のマッチングだけがサポートされています。

class-map match-any *class-map-name* グローバル コンフィギュレーション コマンドを入力した場合、次の **match** コマンドを入力できます。

- **match access-group** *name acl-name*



Note ACL は、名前付き拡張 ACL にする必要があります。

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

match access-group *acl-index* コマンドはサポートされていません。

物理ポート単位でパケット分類を定義するために、クラス マップごとに1つの **match** コマンドのみがサポートされています。この場合、**match-any** キーワードと同じです。

match ip dscp *dscp-list* コマンドまたは **match ip precedence** *ip-precedence-list* コマンドの場合は、よく使用される値のニーモニック名を入力できます。たとえば、**match ip dscp af11** コマンドを入力すると、**match ip dscp 10** コマンドを入力した場合と同じになります。**match ip precedence critical** コマンドを入力すると、**match ip precedence 5** コマンドを入力した場合と同じになります。サポートされているニーモニックの一覧を表示するには、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインのヘルプ文字列を参照してください。

階層ポリシー マップ内にインターフェイス レベルのクラス マップを設定するときには、**input-interface** *interface-id-list* キーワードを使用します。*interface-id-list* には、最大6つのエントリを指定することができます。

Examples

次の例では、クラス マップ **class2** を作成する方法を示します。このマップは、DSCP 値 10、11、および 12 を持つすべての着信トラフィックに一致します。

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

次の例では、クラスマップ **class3** を作成する方法を示します。このマップは、IP precedence 値 5、6、および 7 を持つすべての着信トラフィックに一致します。

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

次の例では、IP precedence 一致基準を削除し、**acl1** を使用してトラフィックを分類する方法を示します。

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

次の例では、階層ポリシーマップでインターフェイスレベルのクラスマップが適用する物理ポートのリストの指定方法を示しています。

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

次の例では、階層ポリシーマップでインターフェイスレベルのクラスマップが適用する物理ポートの範囲の指定方法を示しています。

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

設定を確認するには、**show class-map** 特権 EXEC コマンドを入力します。

policy-map

複数の物理ポートまたはスイッチ仮想インターフェイス（SVI）に適用できるポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **policy-map** コマンドを使用します。既存のポリシー マップを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name ポリシーマップ名です。

Command Default

ポリシー マップは定義されません。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

policy-map コマンドを入力すると、ポリシー マップ クラス コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

- **class:** 指定したクラス マップの分類一致基準を定義します。
- **description:** ポリシー マップを説明します（最大 200 文字）。
- **exit:** ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
- **no:** 定義済みポリシー マップを削除します。
- **sequence-interval:** シーケンス番号機能をイネーブルにします。

グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して作成、追加または変更するポリシー マップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシーマップ コンフィギュレーション モードがイネーブルになり、このモードでポリシー マップのクラス ポリシーを設定または変更することができます。

クラスポリシーをポリシーマップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一貫基準を設定するには、**class-map** グローバル コンフィギュレーション コマンドおよび **match** クラスマップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

サポートされるポリシー マップは、入力ポートに 1 つだけです。複数の物理ポートに対して、同一のポリシーマップを適用することができます。

物理ポートに非階層ポリシーマップを適用できます。非階層ポリシーマップは、デバイスのポートベースポリシーマップと同じです。

階層ポリシー マップには親子ポリシーの形式で 2 つのレベルがあります。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。

VLAN ベースの QoS では、サービス ポリシーが SVI インターフェイスに適用されます。



Note すべての MQS QoS の組み合わせが有線ポートでサポートされているわけではありません。これらの制約事項については、QoS コンフィギュレーションガイドの「Restrictions for QoS on Wired Targets」の章を参照してください。

Examples

次の例では、policy1 という名前のポリシー マップを作成する方法を示します。入力ポートに適用した場合、class1 で定義されたすべての着信トラフィックの照合を行い、IP DSCP を 10 に設定し、平均伝送速度 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイル未滿のトラフィックが送信されます。

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

次に、階層ポリシーを設定する例を示します。

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
```

```
Device(config-pmap-c)# service-policy child  
Deviceconfig-pmap-c)# end
```

次に、ポリシー マップを削除する例を示します。

```
Device(config)# no policy-map policymap2
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

priority

ポリシーマップに属するトラフィックのクラスにプライオリティを割り当てるには、ポリシーマップクラスコンフィギュレーションモードで **priority** コマンドを使用します。クラスに指定したプライオリティを削除するには、このコマンドの **no** 形式を使用します。

```
priority [Kbps [burst -in-bytes] ] | level level-value [Kbps [burst -in-bytes] ] | percent
percentage [Kb/s [burst -in-bytes] ] ]
no priority [Kb/s [burst -in-bytes] ] | level level value [Kb/s [burst -in-bytes] ] | percent
percentage [Kb/s [burst -in-bytes] ] ] ]
```

Syntax Description

<i>Kb/s</i>	(任意) プライオリティトラフィック向けの保証帯域幅 (キロビット/秒 (kbps))。帯域幅の量は、使用中のインターフェイスとプラットフォームによって異なります。保証帯域幅を超えると、非プライオリティトラフィックがなくならないようにするため、プライオリティトラフィックが輻輳のイベントでドロップされます。値は 1 ~ 2,000,000 kbps である必要があります。
<i>burst -in-bytes</i>	(任意) バイト単位のバーストサイズ。バーストサイズは、トラフィックの一時的なバーストに対応するネットワークを設定します。デフォルトバースト値は、設定されている帯域幅レートで、200 ミリ秒のトラフィックとして計算され、burst 引数が指定されていない場合に使用されます。バーストの範囲は 32 ~ 2000000 バイトです。
level level-value	(任意) プライオリティ レベルを割り当てます。level-value の有効値は 1 と 2 です。レベル 1 はレベル 2 よりもプライオリティが高くなります。レベル 1 は帯域幅を予約して最初に送信を行うため、遅延は非常に低くなります。
percent percentage	(任意) 保証帯域幅の量が、使用可能な帯域幅の割合 (%) によって指定されることを、指定します。

Command Default

プライオリティは設定されません。

Command Modes

ポリシーマップクラスコンフィギュレーション (config-pmap-c)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

同じポリシーマップ内では、bandwidth コマンドおよび priority コマンドは、同じクラスに使用できません。ただし、これらのコマンドは、同じポリシーマップ内では一緒に使用できます。

クラスポリシー設定が含まれているポリシーマップがインターフェイスに付加されて、そのインターフェイスのサービス ポリシーが決定される場合、使用可能な帯域幅が評価されます。インターフェイスの帯域幅が不十分なことが原因で、特定のインターフェイスにポリシーマップがアタッチできない場合、そのポリシーは、正常にアタッチされていたすべてのインターフェイスから削除されます。

例

次に、ポリシー マップ `policy1` のクラスのプライオリティを設定する例を示します。

```
Device(config)# class-map cm1
Device(config-cmap)#match precedence 2
Device(config-cmap)#exit

Device(config)#class-map cm2
Device(config-cmap)#match dscp 30
Device(config-cmap)#exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 1m
Device(config-pmap-c-police)#exit
Device(config-pmap-c)#exit
Device(config-pmap)#exit

Device(config)#policy-map policy1
Device(config-pmap)#class cm2
Device(config-pmap-c)#priority level 2
Device(config-pmap-c)#police 1m
```

qos queue-softmax-multiplier

インターフェイスで使用しているソフトバッファの値を増やすには、グローバル コンフィギュレーション モードで **qos queue-softmax-multiplier** コマンドを使用します。

```
qos queue-softmax-multiplier range-of-multiplier
no qos queue-softmax-multiplier range-of-multiplier
```

Syntax Description	<i>range-of-multiplier</i>	値は、100 ~ 1200 の範囲で指定できます。デフォルト値は 100 です。
Command Default	なし	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、softmax バッファの値を 500 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# qos queue-softmax-multiplier 500
```

queue-buffers ratio

クラスのキューバッファを設定するには、ポリシーマップクラスコンフィギュレーションモードで **queue-buffers ratio** コマンドを使用します。比率制限を削除するには、このコマンドの **no** 形式を使用します。

queue-buffers ratio *ratio limit*
no queue-buffers ratio *ratio limit*

Syntax Description	<i>ratio limit</i> (任意) クラスのキューバッファを設定します。キューバッファの比率制限 (0 ~ 100) を入力します。				
Command Default	クラスのキューバッファは定義されていません。				
Command Modes	ポリシーマップクラスコンフィギュレーション (config-pmap-c)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines このコマンドを使用する前に、**bandwidth**、**shape** または **priority** コマンドのいずれかを使用する必要があります。これらのコマンドの詳細については、Cisco.com で入手可能な *Cisco IOS Quality of Service* ソリューションのコマンドリファレンスを参照してください。

デバイスでは、キューにバッファを割り当てることができます。バッファが割り当てられていない場合、すべてのキューの間で均等に分割されます。**queue-buffer ratio** を使用して、特定の比率で分割できます。デフォルトでは、ダイナミックしきい値およびスケージング (DTS) がすべてのキューでアクティブであるため、バッファはソフトバッファです。

例

次にキューバッファの比率を 10% に設定する例を示します。

```
Device(config)# policy-map policy_queuebuf01
Device(config-pmap)# class-map class_queuebuf01
Device(config-cmap)# exit
Device(config)# policy policy_queuebuf01
Device(config-pmap)# class class_queuebuf01
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# queue-buffers ratio 10
Device(config-pmap)# end
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

queue-limit

キューが保持できる、ポリシーマップ内に設定されたクラスポリシーのパケットの最大数を指定または変更するには、**queue-limit** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。クラスからキュー パケット制限を削除するには、このコマンドの **no** 形式を使用します。

```
queue-limit queue-limit-size[packets] {cos cos-value | dscp dscp-value} percent percentage-of-packets
no queue-limit queue-limit-size [packets] {cos cos-value | dscp dscp-value} percent
percentage-of-packets
```

Syntax Description

<i>queue-limit-size</i>	キューの最大サイズ。最大値は、オプションの指定される測定単位用キーワード（bytes、ms、または packets）の単位によって異なります。
cos <i>cos-value</i>	各 cos 値のパラメータを指定します。CoS 値の範囲は 0 ～ 7 です。
dscp <i>dscp-value</i>	各 DSCP 値のパラメータを指定します。 キュー制限のタイプに合わせて DiffServ コードポイント値を指定します。範囲は 0 ～ 63 です。
percent <i>percentage-of-packets</i>	このクラスのキューが蓄積できるパケットの最大割合を指定します。範囲は 1 ～ 100 です。

Command Default

なし

Command Modes

ポリシー マップ クラス コンフィギュレーション（policy-map-c）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

packets 測定単位は、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。**percent** 測定単位を使用してください。



Note このコマンドは、出力方向の有線ポートでのみサポートされています。

Weighted Fair Queuing（WFQ）により、クラス マップが定義される各クラスのキューが作成されます。クラスの一致条件を満たすパケットは、送信されるまで、このクラス専用のキューに蓄積されます。この処理は、均等化キューイングプロセスによってキューが処理される場合に発生し

ます。クラスに定義した最大パケットしきい値に達すると、クラスキューへのそれ以降のパケットのキューイングは、テールドロップされます。

重み付けテールドロップ（WTD）を設定するためにキュー制限を使用します。WTDを使用すると、キューごとに複数のしきい値を設定できます。各サービスクラスが異なるしきい値でドロップされて QoS 差別化が実現されます。

トラフィックの異なるサブクラス、つまり、DSCP と CoS に最大キューしきい値を設定し、各サブクラスに最大キューしきい値を設定できます。

例

次の例では、`dscp-1` というクラスのポリシーを含めるために `port-queue` というポリシーマップを設定しています。このクラスのポリシーは、確保されているキューの最大パケット制限が 20% になるように設定されています。

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```

random-detect cos

サービスクラス (CoS) の値に対する最小と最大の packetsize 値を変更するには、QoS ポリシーマップ クラス コンフィギュレーション モードで **random-detect cos** コマンドを使用します。最小および最大 packetsize 値を CoS 値のデフォルトに戻すには、このコマンドの **no** 形式を使用します。

random-detect cos *cos-value percent min-threshold max-threshold*
no random-detect cos *cos-value percent min-threshold max-threshold*

Syntax Description

<i>cos-value</i>	CoS 値であり、IEEE 802.1Q/ISL のサービス クラス/ユーザ プライオリティ 値です。CoS 値には 0 ~ 7 の数を指定できます。
<i>percent</i>	最小値および packetsize 値がパーセンテージであることを指定します。
<i>min-threshold</i>	パケット数での最小 packetsize 値。この引数に指定できる値の範囲は、1 ~ 512000000 です。キューの平均の長さが最小 packetsize 値に達すると、重み付けランダム早期検出 (WRED) は指定した CoS 値の一部のパケットをランダムにドロップします。
<i>max-threshold</i>	パケット数での最大 packetsize 値。この引数の値の範囲は、 <i>min-threshold</i> 引数の最小値から 512000000 までです。平均キューの長さが最大 packetsize 値を超えると、WRED または DWRED では、指定された CoS の値ですべてのパケットがドロップされます。

Command Modes

QoS ポリシー クラス コンフィギュレーション (config-pmap-c)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

QoS ポリシーマップ クラス コンフィギュレーション モードで **random-detect cos** コマンドと **random-detect** コマンドを併用して使用します。

random-detect cos コマンドは、**random-detect** コマンドをインターフェイス コンフィギュレーション モードで使用しているときに cos ベースの引数を指定した場合にのみ使用できます。

Examples

次に、CoS 値 8 を使用して、WRED をイネーブルにする例を示します。CoS 値 8 の最小 packetsize 値は 20 で、最大 packetsize 値は 40 です。

```
random-detect cos-based
random-detect cos percent 5 20 40
```

Related Commands

コマンド	説明
random-detect	WRED をイネーブルにします。

random-detect cos-based

パケットのサービスクラス (CoS) に基づいて、重み付けランダム早期検出 (WRED) をイネーブルにするには、ポリシーマップクラス コンフィギュレーションモードで **random-detectcos-based** コマンドを使用します。WRED をディセーブルにするには、このコマンドの **no** 形式を使用します。

random-detect cos-based
no random-detect cos-based

Command Default

WRED が設定される場合、最大と最小のしきい値は、出力バッファリング容量とインターフェイスの送信速度に基づいて、決定されます。

Command Modes

ポリシーマップクラス コンフィギュレーション (config-pmap-c)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の例では、CoS 値に基づいて WRED が設定されます。

```
Device> enable
Device# configure terminal
Device(config)# policy-map policymap1
Device(config-pmap)# class class1
Device(config-pmap-c)# random-detect cos-based
Device(config-pmap-c)#

end
```

Related Commands

コマンド	説明
random-detect cos	WRED をイネーブルにするために使用される、パケットの CoS 値、最小しきい値、最大しきい値、最大確率分母を指定します。
show policy-map	指定されたサービスポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
show policy-map interface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスの packets 統計情報を表示します。

random-detect dscp

DiffServ コードポイント（DSCP）の値に対する最小と最大のパケットしきい値を変更するには、QoS ポリシーマップ クラス コンフィギュレーション モードで **random-detect dscp** コマンドを使用します。最小および最大パケットしきい値を DSCP 値のデフォルトに戻すには、このコマンドの **no** 形式を使用します。

random-detect dscp *dscp-value percent min-threshold max-threshold*
no random-detect dscp *dscp-value percent min-threshold max-threshold*

Syntax Description

<i>dscp-value</i>	DSCP 値。DSCP 値には 0 ～ 63 の数値、または次のキーワードのいずれかを指定できます。af11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、cs1、cs2、cs3、cs4、cs5、cs7、ef、または rsvp。
<i>percent</i>	最小値およびしきい値がパーセンテージであることを指定します。
<i>min-threshold</i>	パケット数での最小しきい値。この引数に指定できる値の範囲は、1 ～ 512000000 です。キューの平均の長さが最小しきい値に達すると、重み付けランダム早期検出（WRED）は指定した DSCP 値の一部のパケットをランダムにドロップします。
<i>max-threshold</i>	パケット数での最大しきい値。この引数の値の範囲は、 <i>min-threshold</i> 引数の最小値から 512000000 までです。平均キューの長さが最大しきい値を超えると、WRED または DWRED では、指定された DSCP の値ですべてのパケットがドロップされます。

Command Modes

QoS ポリシー クラス コンフィギュレーション（config-pmap-c）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

QoS ポリシーマップ クラス コンフィギュレーション モードで **random-detect dscp** コマンドと **random-detect** コマンドを併用して使用します。

random-detect dscp コマンドは、**random-detect** コマンドをインターフェイス コンフィギュレーション モードで使用しているときに DSCP ベースの引数を指定した場合にのみ使用できます。

DSCP 値の指定

random-detect dscp コマンドを使用すると、トラフィッククラスごとに DSCP 値を指定できます。DSCP 値には 0 ～ 63 の数値、または次のキーワードのいずれかを指定できます。af11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、cs1、cs2、cs3、cs4、cs5、cs7、ef、または rsvp。

特定のトラフィック クラスでは、トラフィック クラスごとに 8 つの DSCP の値を設定できます。8 つの precedence の値、12 の相対的優先転送 (AF) コードポイント、1 つの完全優先転送コードポイント、8 つのユーザ定義の DSCP の値の、あわせて 29 の値を設定できます。

Assured Forwarding コードポイント

AF コードポイントを使用すると、ドメインで、他のドメイン (カスタマーなど) から受信する IP パケットに対し、4 つの異なるレベル (4 つの異なる AF クラス) の転送保証を利用できるようになります。4 つの AF クラスのそれぞれに、一定の転送サービス (バッファ スペースおよび帯域幅) が割り当てられます。

それぞれの AF クラスでは、IP パケットが、3 つのドロップ precedence の値 (バイナリ 2{010}、4{100}、または 6{110}) の 1 つでマーク付けされます。この 3 つの値は、DSCP ヘッダーの下位 3 つのビットとして存在します。輻輳ネットワーク環境では、パケットのドロップ precedence の値により、AF クラス内のパケットの重要度が決定されます。より高いドロップ precedence の値を持つパケットは、より低いドロップ precedence の値を持つパケットより先に、破棄されます。

DSCP 値の上位 3 ビットにより、AF クラスが決定され、下位 3 ビットにより、破棄確率が決定されます。

Examples

次に、DSCP 値 8 を使用して、WRED をイネーブルにする例を示します。DSCP 値 8 の最小しきい値は 20、最大しきい値は 40、マーク付けの率は 1/10 です。

```
random-detect dscp percent 8 20 40
```

Related Commands

コマンド	説明
random-detect	WRED をイネーブルにします。

random-detect dscp-based

重み付けランダム早期検出（WRED）をパケットのDiffServコードポイント（DSCP）値に基づくようにするには、ポリシーマップクラスコンフィギュレーションモードで **random-detectdscp-based** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

random-detect dscp-based
no random-detect dscp-based

Syntax Description	このコマンドには引数またはキーワードはありません。
Command Default	WRED はデフォルトでディセーブルになっています。
Command Modes	ポリシーマップ クラス コンフィギュレーション (config-pmap-c)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **random-detectdscp-based** コマンドでは、WRED はパケットの DSCP 値に基づきます。
random-detectdscp コマンドを設定する前に **random-detectdscp-based** コマンドを使用します。

Examples

次に、パケットの precedence の値に基づいたランダム検出の例をします。

```
Device> enable
Device# configure terminal
Device(config)#

policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# random-detect dscp-based
Device(config-pmap-c)# random-detect dscp 2 percent 10 40
Device(config-pmap-c)# exit
```

Related Commands

コマンド	説明
random-detect	WRED をイネーブルにします。
random-detect dscp	ポリシーマップ内のクラス ポリシーに対する、特定の DSCP 値の WRED パラメータを設定します。

random-detect precedence

ポリシーマップでクラスポリシーの特定の IP precedence に重み付けランダム早期検出 (WRED) パラメータを設定するには、QoS ポリシーマップ クラス コンフィギュレーション モードで **random-detect precedence** コマンドを使用します。precedence のデフォルトに値を戻すには、このコマンドの **no** 形式を使用します。

random-detect precedence precedence percent min-threshold max-threshold
no random-detect precedence

Syntax Description

<i>precedence</i>	IP precedence 番号。使用できる値の範囲は 0 ~ 7 です。「使用上のガイドライン」の項の表 1 を参照してください。
<i>percent</i>	しきい値がパーセンテージであることを示します。
<i>min-threshold</i>	パケット数での最小しきい値。この引数に指定できる値の範囲は、1 ~ 512000000 です。平均キューの長さが最小しきい値に達すると、WRED では、指定された IP precedence で一部のパケットがランダムにドロップされます。
<i>max-threshold</i>	パケット数での最大しきい値。この引数の値の範囲は、 <i>min-threshold</i> 引数の最小値から 512000000 までです。平均キューの長さが最大しきい値を超えると、WRED または DWRED では、指定された IP precedence の値ですべてのパケットがドロップされます。

Command Default

デフォルトの *min-threshold* 値は precedence の値に応じて異なります。IP precedence 0 の *min-threshold* の値は、*max-threshold* の値の半分になります。残りの precedence 値は、*max-threshold* の値の半分から *max-threshold* の値までの間に、等間隔に配置されます。各 IP precedence のデフォルトの最小しきい値の一覧については、このコマンドの「使用上のガイドライン」のセクションにある表を参照してください。

Command Modes

インターフェイス コンフィギュレーション (config-if)

QoS ポリシー クラス コンフィギュレーション (config-pmap-c)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

WRED は、輻輳が存在するときにランダムにパケットをドロップすることでトラフィックを遅くする輻輳回避メカニズムです。

インターフェイスで **random-detect** コマンドを設定すると、パケットの IP precedence に基づいて、パケットに対する優先処理が行われます。異なる precedence に対する処理を調節するには、**random-detect precedence** コマンドを使用します。

WRED でドロップするパケットを決定する際に IP precedence を無視する場合は、各 IP precedence に同じパラメータでこのコマンドを入力します。最小しきい値および最大しきい値には、適切な値を設定します。

random-detect precedence コマンドを使用してクラスポリシー内の異なる precedence に対する処理を調節する場合、そのサービスポリシーを適用するインターフェイスに WRED が設定されていないことを確認する必要があります。



Note *min-threshold* 引数と *max-threshold* 引数の値の範囲は 1 ~ 512000000 ですが、指定可能な実際の値は設定するランダム検出のタイプに応じて異なります。たとえば、最大しきい値がキューの制限を超えることはできません。

Examples

次に、インターフェイスで WRED をイネーブルにし、さまざまな IP precedence にパラメータを指定する設定例を示します。

```
interface FortyGigE1/0/1
  description 45Mbps to R1
  ip address 10.200.14.250 255.255.255.252
  random-detect
  random-detect precedence 7 percent 20 50
```

Related Commands

コマンド	説明
bandwidth (policy-map class)	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
random-detect dscp	DSCP 値の最小および最大パケットしきい値を変更します。
show policy-map interface	指定されたインターフェイスのすべてのサービスポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定の PVC に対するサービスポリシーのクラスを表示します。
show queuing	すべてまたは選択した設定済みキューイング戦略を表示します。

random-detect precedence-based

重み付けランダム早期検出（WRED）をパケットの precedence 値に基づくようにするには、ポリシーマップクラス コンフィギュレーション モードで **random-detect precedence-based** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

random-detect precedence-based
no random-detect precedence-based

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

WRED はデフォルトでディセーブルになっています。

Command Modes

ポリシーマップクラス コンフィギュレーション（config-pmap-c）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

random-detect precedence-based コマンドでは、WRED はパケットの IP precedence 値に基づきます。

random-detect precedence-based コマンドを設定する前に **random-detect precedence-based** コマンドを使用します。

Examples

次に、パケットの precedence の値に基づいたランダム検出の例をします。

```
Device> enable
Device# configure terminal
Device(config)#

policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# random-detect precedence-based
Device(config-pmap-c)# random-detect precedence 2 percent 30 50
Device(config-pmap-c)# exit
```

Related Commands

コマンド	説明
random-detect	WRED をイネーブルにします。
random-detect precedence	ポリシーマップ内のクラス ポリシーに対する、特定の IP precedence の WRED パラメータを設定します。

service-policy (有線)

物理ポートまたはスイッチ仮想インターフェイス (SVI) にポリシーマップを適用するには、インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用します。ポリシーマップとポートの対応付けを削除するには、このコマンドの **no** 形式を使用します。

```
service-policy {input | output} policy-map-name
no service-policy {input | output} policy-map-name
```

Syntax Description

input *policy-map-name* 物理ポートまたはSVIの入力に、指定したポリシーマップを適用します。

output *policy-map-name* 物理ポートまたはSVIの出力に、指定したポリシーマップを適用します。

Command Default

ポートにポリシーマップは適用されていません。

Command Modes

WLAN インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ポリシーマップは、**policy map** コマンドによって定義されます。

1つのポートごとに入力と出力に関して1つのポリシーマップだけがサポートされます。つまり、いずれのポートにおいても、1つの入力ポリシーと1つの出力ポリシーだけを使用できます。

ポリシーマップは、物理ポートまたは SVI 上の着信トラフィックに適用できます。

Examples

次の例では、物理入力ポートに **plcmap1** を適用する方法を示します。

```
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# service-policy input plcmap1
```

次の例では、物理ポートから **plcmap2** を削除する方法を示します。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# no service-policy input plcmap2
```

次の例では、VLAN のポリサー設定を表示します。この設定の最後に、QoS のインターフェイスに VLAN ポリシーマップを適用します。

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
```

```
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/5
Device(config-if)# service-policy input vlan100
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

set

パケットで DiffServ コード ポイント (DSCP) 値または IP precedence 値を設定して IP トラフィックを分類するには、ポリシーマップ クラス コンフィギュレーション モードで **set** コマンドを使用します。トラフィックの分類を削除するには、このコマンドの **no** 形式を使用します。

set

cos | dscp | precedence | ip | qos-group

set cos

{*cos-value*} | {**cos | dscp | precedence | qos-group**} [**table** *table-map-name*]

set dscp

{*dscp-value*} | {**cos | dscp | precedence | qos-group**} [**table** *table-map-name*]

set ip {dscp | precedence}

set precedence {*precedence-value*} | {**cos | dscp | precedence | qos-group**} [**table** *table-map-name*]

set qos-group

{*qos-group-value* | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]}

Syntax Description

cos

発信パケットのレイヤ 2 サービス クラス (CoS) 値またはユーザプライオリティを設定します。次の値を指定できます。

- **cos-value:** 0 ~ 7 の CoS 値。一般的に使用する値に対してはニーモニック名を入力することもできます。
- パケットに CoS 値を設定するためのパケットマーキングカテゴリを指定します。パケットマーキング値をマッピングおよび変換するためのテーブルマップも設定している場合は、これによって「map from」パケットマーキングカテゴリが確立されます。パケットマーキングカテゴリのキーワードは次のとおりです。
 - **cos:** CoS 値またはユーザプライオリティからの値を設定します。
 - **dscp:** DiffServ コードポイント (DSCP) からの値を設定します。
 - **precedence:** パケット優先順位からの値を設定します。
 - **qos-group:** QoS グループからの値を設定します。
- (任意) **table table-map-name:** CoS 値の設定に使用される指定されたテーブルマップに設定されている値を示します。CoS 値の指定に使用されるテーブルマップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。

パケットマーキングカテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキングカテゴリに関連付けられた値を CoS 値としてコピーすることです。たとえば、**set cos precedence** コマンドを入力する場合、**precedence** (パケットマーキングカテゴリ) 値がコピーされ、CoS 値として使用されます。

dscp

IP (v4) および IPv6 パケットの DiffServ コードポイント (DSCP) を指定します。次の値を指定できません。

- **cos-value:** DSCP 値を設定する番号。範囲は 0 ~ 63 です。一般的に使用する値に対してはニック名を入力することもできます。
- パケットに DSCP 値を設定するためのパケットマーキングカテゴリを指定します。パケットマーキング値をマッピングおよび変換するためのテーブルマップも設定している場合は、これによって「map from」パケットマーキングカテゴリが確立されます。パケットマーキングカテゴリのキーワードは次のとおりです。
 - **cos:** CoS 値またはユーザプライオリティからの値を設定します。
 - **dscp:** DiffServ コードポイント (DSCP) からの値を設定します。
 - **precedence:** パケット優先順位からの値を設定します。
 - **qos-group:** QoS グループからの値を設定します。
- (任意) **table table-map-name:** DSCP 値の設定に使用される指定されたテーブルマップに設定されている値を示します。DSCP 値の指定に使用されるテーブルマップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。

パケットマーキングカテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキングカテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、**set dscp cos** コマンドを入力する場合、CoS 値 (パケットマーキングカテゴリ) がコピーされ、DSCP 値として使用されます。

ip

分類されたトラフィックに IP 値を設定します。次の値を指定できます。

- **dscp:** 0～63 の IP DSCP 値またはパケットマーキングカテゴリを指定します。
- **precedence:** IP ヘッダーの precedence ビット値を指定します（有効な値は 0～7）。または、パケットマーキングカテゴリを指定します。

precedence

パケットヘッダーに precedence 値を設定します。次の値を指定できます。

- **precedence-value:** パケットヘッダーに precedence ビットを設定します。有効な値は 0～7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
- パケットの優先順位値を設定するためのパケットマーキングカテゴリを指定します。
 - **cos:** CoS またはユーザプライオリティからの値を設定します。
 - **dscp:** DiffServ コードポイント (DSCP) からの値を設定します。
 - **precedence:** パケット優先順位からの値を設定します。
 - **qos-group:** QoS グループからの値を設定します。
- (任意) **table table-map-name:** 優先順位値の設定に使用される指定されたテーブルマップに設定されている値を示します。優先順位値の指定に使用されるテーブルマップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。

パケットマーキングカテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキングカテゴリに関連付けられた値を優先順位値としてコピーすることです。たとえば、**set precedence cos** コマンドを入力する場合、CoS 値（パケットマーキングカテゴリ）がコピーされ、precedence 値として使用されます。

qos-group

後でパケットを分類するために使用できる QoS グループ ID を割り当てます。

- **qos-group-value:** 分類されたトラフィックに QoS 値を設定します。指定できる範囲は 0 ~ 31 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
- **dscp:** パケットの元の DSCP フィールド値を QoS グループ値として設定します。
- **precedence:** パケットの元の precedence フィールド値を QoS グループ値として設定します。
- (任意) **table table-map-name:** DSCP 値または優先順位値の設定に使用される指定されたテーブルマップに設定されている値を示します。値の指定に使用されるテーブルマップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。

パケットマーキングカテゴリ (**dscp** または **precedence**) を指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキングカテゴリに関連付けられた値を QoS グループ値としてコピーすることです。たとえば、**set qos-group precedence** コマンドを入力する場合、precedence 値 (パケットマーキングカテゴリ) がコピーされ、QoS グループ値として使用されます。

Command Default

トラフィックの分類は定義されていません。

Command Modes

ポリシー マップ クラス コンフィギュレーション

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入さ

Usage Guidelines

set dscp dscp-value コマンド、**set cos cos-value** コマンド、および **set ip precedence precedence-value** コマンドの場合は、一般に使用されている値のニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力すると、**set dscp 10** コマンドを入力した場合と同じになります。**set ip precedence critical** コマンドを入力すると、**set ip precedence 5** コマンドを入力した場合と同じになります。サポートされているニーモニックの一覧を表示するには、**set dscp ?** または **set ip precedence ?** コマンドを入力して、コマンドラインのヘルプ文字列を参照してください。

set dscp cos コマンドを設定する場合は、CoS 値が 3 ビット フィールドで、DSCP 値は 6 ビット フィールドであり、CoS フィールドの 3 ビットのみが使用される点に注意してください。

set dscp qos-group コマンドを設定する場合は、次の点に注意してください。

- DSCP 値の有効な範囲は 0 ~ 63 の数字です。QoS グループの有効値の範囲は 0 ~ 99 です。
- QoS グループの値が両方の値の範囲内の場合（たとえば、44）、パケットマーキング値がコピーされ、パケットがマーク付けされます。
- QoS グループの値が DSCP の範囲を超える場合（たとえば、77）、パケットマーキング値はコピーされず、パケットはマーク付けされません。アクションは実行されません。

ポリシーマップコンフィギュレーションモードでサービスポリシーを作成し、インターフェイスまたは ATM 仮想回線（VC）にサービスポリシーを付加するまで、**set qos-group** コマンドは適用できません。

ポリシーマップ コンフィギュレーションモードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

Examples

次の例では、ポリサーが設定されていないすべての FTP トラフィックに DSCP 値 10 を割り当てる方法を示します。

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

show auto qos

automatic QoS (auto-QoS) が有効になっているインターフェイスに入力された Quality of Service (QoS) コマンドを表示するには、特権 EXEC モードで **show auto qos** コマンドを使用します。

show auto qos [**interface** *interface-id*]

Syntax Description	interface (任意) 指定されたポートまたはすべてのポートの auto-QoS 情報を表示し <i>[interface-id]</i> ます。有効なインターフェイスには、物理ポートが含まれます。
Command Modes	ユーザ EXEC 特権 EXEC
Command History	リリース 変更内容 Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

Usage Guidelines **show auto qos** コマンド出力には、各インターフェイスに入力された **auto qos** コマンドだけが表示されます。**show auto qos interface interface-id** コマンド出力には、特定のインターフェイス上に入力された **auto qos** コマンドが表示されます。

auto-QoS 設定およびユーザ変更を表示する場合は、**show running-config** 特権 EXEC コマンドを使用します。

Examples

次の例では、**auto qos voip cisco-phone** および **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos** コマンドの出力を示します。

```
Device# show auto qos
GigabitEthernet 2/0/4
auto qos voip cisco-softphone
```

```
GigabitEthernet 2/0/5
auto qos voip cisco-phone
```

```
GigabitEthernet 2/0/6
auto qos voip cisco-phone
```

次に、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドが入力された場合の **show auto qos interface interface-id** コマンドの出力例を示します。

```
Device# show auto qos interface GigabitEthernet 2/0/5
GigabitEthernet 2/0/5
auto qos voip cisco-phone
```

次の例では、auto-QoS がインターフェイスでディセーブルになっている場合の **show auto qos interface interface-id** コマンドの出力を示します。

```
Device# show auto qos interface GigabitEthernet 3/0/1
AutoQoS is disabled
```

show class-map

トラフィックを分類するための一致基準を定義するサービス品質（QoS）クラス マップを表示するには、**show class-map** コマンドを EXEC モードで使用します。

show class-map [*class-map-name* | **type control subscriber** {**all** | *class-map-name*}]

Syntax Description

class-map-name (任意) クラス マップ名。

type control subscriber (任意) コントロール クラス マップに関する情報を表示します。

all (任意) すべてのコントロール クラス マップに関する情報を表示します。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Examples

次に、**show class-map** コマンドの出力例を示します。

```
Device# show class-map
Class Map match-any videowizard_10-10-10-10 (id 2)
  Match access-group name videowizard_10-10-10-10

Class Map match-any class-default (id 0)
  Match any

Class Map match-any dscp5 (id 3)
  Match ip dscp 5
```

show platform hardware fed switch

デバイス固有のハードウェア情報を表示するには、**show platform hardware fed switch** *switch_number* コマンドを使用します。

このトピックでは、QoS特有のオプション、つまり **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **qos** コマンドで使用可能なオプションのみについて詳しく説明します。

```
show platform hardware fed switch {switch_num | active | standby} qos {afd | {config type type | [asic
asic_num] | stats clients {all | bssid id | wlanid id}} | dscp-cos counters {iifd_id id | interface type number}
| le-info | {iifd_id id | interface type number} | policer config {iifd_id id | interface type number} | queue
| {config | {iifd_id id | interface type number | internal port-type type {asic number [port_num]}} |
label2qmap | [aqmrepqostbl | iqslabtable | sqslabtable] | {asic number} | stats | {iifd_id id | interface
type number | internal {cpu policer | port-type type asic number} {asic number [port_num]}}} | resource}
```

Syntax Description

switch { <i>switch_num</i> active standby }	<p>情報を表示するスイッチ。次の選択肢があります。</p> <ul style="list-style-type: none"> • switch_num: スイッチの ID。 • active: アクティブなスイッチに関する情報を表示します。 • standby: 存在する場合、スタンバイスイッチに関する情報を表示します。
qos	<p>QoS ハードウェア情報を表示します。次のオプションの中から選択する必要があります。</p> <ul style="list-style-type: none"> • afd: ハードウェアの Approximate Fair Drop (AFD) の情報を表示します。 • dscp-cos: 各ポートの DSCP-COS カウンタの情報を表示します。 • leinfo: 論理エンティティ情報を表示します。 • policer: ハードウェアの QoS ポリサー情報を表示します。 • queue: ハードウェアのキュー情報を表示します。 • resource: ハードウェアのリソース情報を表示します。

afd { **config type** | **config type** または **stats client** のオプションから選択する必要があります。
stats client }

config type:

- **client:** ワイヤレス クライアント情報を表示します。
- **port:** ポート固有の情報を表示します。
- **radio:** ワイヤレス無線情報を表示します。
- **ssid:** ワイヤレス SSID 情報を表示します。

stats client :

- **all:** すべてのクライアントの統計を表示します。
- **bssid:** 有効な範囲は 1 ~ 4294967295 です。
- **wlanid:** 有効な範囲は 1 ~ 4294967295 です。

asicasic_num (任意) ASIC 番号。有効な範囲は 0 ~ 255 です。

dscp-cos counters { ポートごとの DSCP-COS カウンタを表示します。 **dscp-cos counters** の次の
iif_id id | オプションから選択する必要があります。
interface type number
}

- **iif_id id:** ターゲットインターフェイスの ID です。有効な範囲は 1 ~ 4294967295 です。
- **interface type number:** ターゲットインターフェイスのタイプおよび ID です。

leinfo **dscp-cos counters** の次のオプションから選択する必要があります。

- **iif_id id:** ターゲットインターフェイスの ID です。有効な範囲は 1 ~ 4294967295 です。
- **interface type number:** ターゲットインターフェイスのタイプおよび ID です。

policer config ハードウェアのポリサーに関連する設定情報を表示します。次のオプションの中から選択する必要があります。

- **iif_id id:** ターゲットインターフェイスの ID です。有効な範囲は 1 ~ 4294967295 です。
 - **interface type number:** ターゲットインターフェイスのタイプおよび ID です。
-

<pre>queue {config {iif_id id interface type number internal} label2qmap stats}</pre>	<p>ハードウェアのキュー情報を表示します。次のオプションの中から選択する必要があります。</p> <ul style="list-style-type: none"> • config: 設定情報です。次のオプションの中から選択する必要があります。 <ul style="list-style-type: none"> • iif_id id: ターゲットインターフェイスの ID です。有効な範囲は 1 ~ 4294967295 です。 • interface type number: ターゲットインターフェイスのタイプおよび ID です。 • internal: 内部キューの関連情報を表示します。 • label2qmap: キューマッピング情報にハードウェアラベルを表示します。次のオプションの中から選択できます。 <ul style="list-style-type: none"> • (任意) aqmreqpostbl: AQM REP QoS ラベルテーブルのルックアップ。 • (任意) iqslabelltable: IQS QoS ラベルテーブルのルックアップ。 • (任意) sqslabelltable: SQS およびローカル QoS ラベルテーブルのルックアップ。 • stats: キューの統計情報を表示します。次のオプションの中から選択する必要があります。 <ul style="list-style-type: none"> • iif_id id: ターゲットインターフェイスの ID です。有効な範囲は 1 ~ 4294967295 です。 • interface type number: ターゲットインターフェイスのタイプおよび ID です。 • internal {cpu policer port_type port_type asic asic_num [port_num port_num] }: 内部キューの関連情報を表示します。
<pre>resource</pre>	<p>ハードウェアリソースの使用情報を表示します。次のキーワードを入力する必要があります。 usage</p>

Command Modes

ユーザ EXEC
特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、`show platform hardware fed switch switch_number qos queue stats internal cpu policer` コマンドの出力例を示します。

```
Device#show platform hardware fed switch 3 qos queue stats internal cpu policer
```

QId	PlcIdx	Queue Name	Enabled	(default) Rate	(set) Rate	Drop
0	11	DOT1X Auth	No	1000	1000	0
1	1	L2 Control	No	500	500	0
2	14	Forus traffic	No	1000	1000	0
3	0	ICMP GEN	Yes	200	200	0
4	2	Routing Control	Yes	1800	1800	0
5	14	Forus Address resolution	No	1000	1000	0
6	3	ICMP Redirect	No	500	500	0
7	6	WLESS PRI-5	No	1000	1000	0
8	4	WLESS PRI-1	No	1000	1000	0
9	5	WLESS PRI-2	No	1000	1000	0
10	6	WLESS PRI-3	No	1000	1000	0
11	6	WLESS PRI-4	No	1000	1000	0
12	0	BROADCAST	Yes	200	200	0
13	10	Learning cache ovfl	Yes	100	100	0
14	13	Sw forwarding	Yes	1000	1000	0
15	8	Topology Control	No	13000	13000	0
16	12	Proto Snooping	No	500	500	0
17	16	DHCP Snooping	No	1000	1000	0
18	9	Transit Traffic	Yes	500	500	0
19	10	RPF Failed	Yes	100	100	0
20	15	MCAST END STATION	Yes	2000	2000	0
21	13	LOGGING	Yes	1000	1000	0
22	7	Punt Webauth	No	1000	1000	0
23	10	Crypto Control	Yes	100	100	0
24	10	Exception	Yes	100	100	0
25	3	General Punt	No	500	500	0
26	10	NFL SAMPLED DATA	Yes	100	100	0
27	2	SGT Cache Full	Yes	1800	1800	0
28	10	EGR Exception	Yes	100	100	0
29	16	Show frwd	No	1000	1000	0
30	9	MCAST Data	Yes	500	500	0
31	10	Gold Pkt	Yes	100	100	0

show platform software fed switch qos

デバイス固有のソフトウェア情報を表示するには、**show platform hardware fed switch *switch_number*** コマンドを使用します。

このトピックでは、**show platform software fed switch {*switch_num* | active | standby } qos** コマンドで使用可能な QoS 特有のオプションのみについて詳しく説明します。

show platform software fed switch {*switch number* | active | standby } qos {*avc* | internal | label2qmap | nflqos | policer | policy | qsb | tablemap}

Syntax Description

switch 情報を表示するデバイス。
{*switch_num* | **active** | **standby** }

- **switch_num**: スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。
- **active**: アクティブスイッチの情報を表示します。
- **standby**: 存在する場合、スタンバイスイッチの情報を表示します。

qos QoS ソフトウェア情報を表示します。次のいずれかのオプションを選択します。

- **avc**: Application Visibility and Control (AVC) QoS 情報を表示します。
- **internal**: 内部キュー関連情報を表示します。
- **label2qmap**: ラベルとキューのマップテーブル情報を表示します。
- **nflqos**: NetFlow QoS 情報を表示します。
- **policer**: ハードウェアの QoS ポリサー情報を表示します。
- **policy**: QoS ポリシー情報を表示します。
- **qsb**: QoS サブブロック情報を表示します。
- **tablemap**: QoS 出力および入力キューのテーブルマッピング情報を表示します。

Command Modes

ユーザ EXEC
特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

show platform software fed switch qos qsb

QoS サブブロック情報を表示するには、**show platform software fed switch *switch_number* qos qsb** コマンドを使用します。

```
show platform software fed switch {switch number | active | standby} qos qsb {brief | [all | type |
{client client_id | port port_number | radio radio_type | ssid ssid}] | iif_id id | interface |
{Auto-Template interface_number | BDI interface_number | Capwap interface_number |
GigabitEthernet interface_number | InternalInterface interface_number | Loopback interface_number |
Null interface_number | Port-channel interface_number | TenGigabitEthernet interface_number |
Tunnel interface_number | Vlan interface_number}}
```

Syntax Description

switch { <i>switch_num</i> active standby }	<p>情報を表示するスイッチ。</p> <ul style="list-style-type: none"> • switch_num: スイッチの ID を入力します。指定されたスイッチに関する情報を表示します。 • active: アクティブスイッチの情報を表示します。 • standby: 存在する場合、スタンバイスイッチの情報を表示します。
qos qsb	QoS サブブロック ソフトウェア情報を表示します。

**qsb {brief | iif_id brief
| interface}**

- **all:** すべてのクライアントの情報を表示します。
- **type:** 指定されたターゲット タイプの qsb 情報を表示します。
 - **client:** ワイヤレス クライアントの QoS qsb 情報を表示します。
 - **port:** ポート固有の情報を表示します。
 - **radio:** ワイヤレス無線の QoS qsb 情報を表示します。
 - **ssid:** ワイヤレス ネットワークの QoS qsb 情報を表示します。

iif_id: iif_ID の情報を表示します。

interface: 指定されたインターフェイスの QoS qsb 情報を表示します。

- **Auto-Template:** 1 ~ 999 の自動テンプレート インターフェイス。
- **BDI:** 1 ~ 16000 のブリッジドメイン インターフェイス。
- **Capwap:** 0 ~ 2147483647 の CAPWAP インターフェイス。
- **GigabitEthernet:** 0 ~ 9 の GigabitEthernet インターフェイス。
- **InternalInterface:** 0 ~ 9 の内部インターフェイス。
- **Loopback:** 0 ~ 2147483647 のループバック インターフェイス。
- **Null:** ヌル インターフェイス 0 ~ 0。
- **Port-Channel:** 1 ~ 128 の port-channel インターフェイス。
- **TenGigabitEthernet:** 0 ~ 9 の TenGigabitEthernet インターフェイス。
- **Tunnel:** 0 ~ 2147483647 のトンネル インターフェイス。
- **Vlan:** 1 ~ 4094 の VLAN インターフェイス。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

このコマンドが導入されました。

次に、**show platform software fed switchswitch_numberqos qsb** コマンドの出力例を示します。

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2
```

```
QoS subblock information:
Name:GigabitEthernet3/0/2 iif_id:0x0000000000007b iif_type:ETHER(146)
qsb ptr:0xffd8573350
```

```

Port type = Wired port
asic_num:0 is_uplink:false init_done:true
FRU events: Active-0, Inactive-0
def_qos_label:0 def_le_priority:13
trust_enabled:false trust_type:TRUST_DSCP ifm_trust_type:1
LE priority:13 LE trans_index(in, out): (0,0)
Stats (plc,q) export counters (in/out): 0/0
Policy Info:
  Ingress Policy: pmap::{(0xffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,)}
    tcg::{(0xffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
status:VALID,SET_INHW
  Egress Policy: pmap::{(0xffd86857d0,AutoQos-4.0-Output-Policy,1076629088,)}
    tcg::{(0xffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
status:VALID,SET_INHW
  TCG(in,out):(0xffd867ad10, 0xffd8685b40) le_label_id(in,out):(2, 1)
Policer Info:
  num_ag_policers(in,out)[1r2c,2r3c]: ([0,0],[0,0])
  num_mf_policers(in,out): (0,0)
  num_afd_policers:0
  [ag_plc_handle(in,out) = (0xd8688220,0)]
  [mf_plc_handle(in,out)=(nil),(nil)] num_mf_policers:(0,0)
  base:(0xffffffff,0xffffffff) rc:(0,0)]
Queueing Info:
  def_queueing = 0, shape_rate:0 interface_rate_kbps:1000000
  Port shaper:false
  lbl_to_qmap_index:1
  Physical qparams:
    Queue Config: NodeType:Physical Id:0x40000049 parent:0x40000049 qid:0 attr:0x1 defq:0

    PARAMS: Excess Ratio:1 Min Cir:1000000 QBuffer:0
    Queue Limit Type:Single Unit:Percent Queue Limit:44192
    SHARED Queue

```

show policy-map

着信トラフィックの分類基準を定義するサービス品質（QoS）のポリシーマップを表示するには、EXEC モードで **show policy-map** コマンドを使用します。

```
show policy-map [ policy-map-name | interface interface-id ]
```

```
show policy-map interface { Auto-template | Capwap | GigabitEthernet | GroupVI |
InternalInterface | Loopback | Lspvif | Null | Port-channel | TenGigabitEthernet | Tunnel
| Vlan | brief | class | input | output }
```

Syntax Description	<i>policy-map-name</i> (任意) ポリシーマップの名前。	
	interface <i>interface-id</i> (任意) インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。	
Command Modes	ユーザ EXEC 特権 EXEC	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマン
Usage Guidelines	ポリシーマップには、帯域幅制限および制限を超過した場合の対処法を指定するポリサーを格納できます。	



Note **control-plane**、**session**、および **type** キーワードは、コマンドラインのヘルプストリングには表示されますが、サポートされていません。表示されている統計情報は無視してください。

次に、**show policy-map interface** コマンドの出力例を示します。

```
Device# show policy-map interface gigabitethernet 1/0/48

Service-policy output: port_shape_parent

Class-map: class-default (match-any)
 191509734 packets
 Match: any
 Queueing

 (total drops) 524940551420
 (bytes output) 14937264500
 shape (average) cir 2500000000, bc 2500000, be 2500000
 target shape rate 250000000

Service-policy : child_trip_play
```

```
queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 524940551420
  (bytes output) 14937180648

queue stats for all priority classes:
  Queueing
  priority level 2

  (total drops) 0
  (bytes output) 0

Class-map: dscp56 (match-any)
  191508445 packets
  Match:  dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: Strict,

  Priority Level: 1
  police:
    cir 10 %
    cir 25000000 bps, bc 781250 bytes
    conformed 0 bytes; actions: >>>>counters not supported
    transmit
    exceeded 0 bytes; actions:
    drop
    conformed 0000 bps, exceeded 0000 bps >>>>counters not supported
```

show tech-support qos

テクニカルサポートに使用する Quality of Service (QoS) 関連の情報を表示するには、特権 EXEC モードで **show tech-support qos** コマンドを使用します。

```
show tech-support qos [switch {switch-number | active | all | standby} | [control-plane | interface { interface-name | all}]]
```

Syntax Description		
switch <i>switch-number</i>		(任意) 特定のスイッチの QoS 関連情報を表示します。
active		(任意) スイッチのアクティブインスタンスの QoS 関連情報を表示します。
all		(任意) スイッチのすべてのインスタンスの QoS 関連情報を表示します。
standby		(任意) スイッチのスタンバイインスタンスの QoS 関連情報を表示します。
control-plane		(任意) コントロールプレーンの QoS 関連情報を表示します。
interface <i>interface-name</i>		(任意) 指定したインターフェイスの QoS 関連情報を表示します。
all		(任意) すべてのインターフェイスの QoS 関連情報を表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Usage Guidelines このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします (たとえば、**show tech-support qos | redirect flash:filename**)。

show tech-support qos コマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なります。

Examples

次に、**show tech-support qos** コマンドの出力例を示します。

```
Device# show tech-support qos
.
.
.
----- show platform software fed switch 1 qos policy target brief
-----

TCG summary for policy: system-cpp-policy

Loc Interface                IIF-ID                Dir tccg Child #m/p/q  State:(cfg,opr)
-----
?:255 Control Plane          0x00000001000001 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4da31c8
?:0 CoPP-Queue-0             0x0000000100000d OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4da41e8
?:0 CoPP-Queue-1             0x0000000100000e OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dbede8
?:0 CoPP-Queue-2             0x0000000100000f OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dc2df8
?:0 CoPP-Queue-3             0x00000001000010 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dc6e08
?:0 CoPP-Queue-4             0x00000001000011 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dcae18
?:0 CoPP-Queue-5             0x00000001000012 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dcee28
?:0 CoPP-Queue-6             0x00000001000013 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dd2e38
?:0 CoPP-Queue-7             0x00000001000014 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dd6e48
?:0 CoPP-Queue-8             0x00000001000015 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4ddae58
?:0 CoPP-Queue-9             0x00000001000016 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4ddee68
?:0 CoPP-Queue-10            0x00000001000017 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4de2e78
?:0 CoPP-Queue-11            0x00000001000018 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4de6e88
?:0 CoPP-Queue-12            0x00000001000019 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4deae98
?:0 CoPP-Queue-13            0x0000000100001a OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4deeea8
?:0 CoPP-Queue-14            0x0000000100001b OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4df2eb8
?:0 CoPP-Queue-15            0x0000000100001c OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4df6ec8
?:0 CoPP-Queue-16            0x0000000100001d OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dfaed8
?:0 CoPP-Queue-17            0x0000000100001e OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4dffee8
?:0 CoPP-Queue-18            0x0000000100001f OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e02ef8
?:0 CoPP-Queue-19            0x00000001000020 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e06f08
?:0 CoPP-Queue-20            0x00000001000021 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e0ae88
?:0 CoPP-Queue-21            0x00000001000022 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e0ee98
?:0 CoPP-Queue-22            0x00000001000023 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e12ea8
?:0 CoPP-Queue-23            0x00000001000024 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e16eb8
?:0 CoPP-Queue-24            0x00000001000025 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e1aec8
?:0 CoPP-Queue-25            0x00000001000026 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e1eed8
?:0 CoPP-Queue-26            0x00000001000027 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e22ee8
?:0 CoPP-Queue-27            0x00000001000028 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e26ef8
?:0 CoPP-Queue-28            0x00000001000029 OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e2af08
?:0 CoPP-Queue-29            0x0000000100002a OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e2ef18
?:0 CoPP-Queue-30            0x0000000100002b OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e32f28
?:0 CoPP-Queue-31            0x0000000100002c OUT  22    0 0/17/0  VALID,SET_INHW  0xffe4e36f38

----- show platform software fed switch 1 qos policy summary -----

Policymap Summary: (counters)
  CGID      Classes Targets Child CfgErr InHw  OpErr Policy Name
-----
15212688   22      33      0      0      33    0      system-cpp-policy
.
.
.
```

出力フィールドの意味は自明です。

trust device

インターフェイスに接続されているサポートデバイスに対する信頼を設定するには、インターフェイス コンフィギュレーション モードで **trust device** コマンドを使用します。接続デバイスに対する信頼を無効にするには、このコマンドの **no** 形式を使用します。

```
trust device {cisco-phone | cts | ip-camera | media-player}
no trust device {cisco-phone | cts | ip-camera | media-player}
```

Syntax Description

cisco-phone	Cisco IP Phone を設定します。
cts	Cisco TelePresence System を設定します。
ip-camera	Video Surveillance IP カメラ (IPVSC) を設定します。
media-player	Cisco Digital Media Player (DMP) を設定します。

Command Default

信頼はディセーブルに設定

Command Modes

インターフェイス コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

trust device コマンドは、次のタイプのインターフェイスに使用します。

- **Auto:** 自動テンプレート インターフェイス
- **Capwap:** Capwap トンネル インターフェイス
- **GigabitEthernet:** Gigabit Ethernet IEEE 802
- **GroupVI:** グループ仮想インターフェイス
- **Internal Interface:** 内部インターフェイス
- **Loopback:** ループバック インターフェイス
- **Null:** スル インターフェイス
- **Port-channel:** イーサネット チャンネル インターフェイス
- **TenGigabitEthernet:** 10 ギガビット イーサネット
- **Tunnel:** トンネル インターフェイス
- **Vlan:** Catalyst VLAN

- range: **interface range** コマンド

例

次に、インターフェイス GigabitEthernet 1/0/1 で Cisco IP 電話の信頼を設定する例を示します。

```
Device(config)# interface gigabitethernet 1/0/1  
Device(config-if)# trust device cisco-phone
```



PART IX

ルーティング

- [IP ルーティングコマンド](#), on page 1223



IP ルーティングコマンド

- [accept-lifetime](#), on page 1225
- [address-family ipv6 \(OSPF\)](#), on page 1228
- [area nssa](#), on page 1229
- [area virtual-link](#), on page 1231
- [authentication \(BFD\)](#), on page 1235
- [bfd](#), on page 1236
- [bfd all-interfaces](#), on page 1238
- [bfd check-ctrl-plane-failure](#), on page 1239
- [bfd echo](#), on page 1240
- [bfd slow-timers](#), on page 1242
- [bfd template](#), on page 1244
- [bfd-template single-hop](#), on page 1245
- [default-information originate \(OSPF\)](#), on page 1246
- [distance \(OSPF\)](#), on page 1248
- [eigrp log-neighbor-changes](#), on page 1251
- [eigrp log-neighbor-warnings](#), on page 1253
- [ip authentication key-chain eigrp](#), on page 1255
- [ip authentication mode eigrp](#), on page 1256
- [ip bandwidth-percent eigrp](#), on page 1258
- [ip cef load-sharing algorithm](#), on page 1259
- [ip prefix-list](#), on page 1260
- [ip hello-interval eigrp](#), on page 1264
- [ip hold-time eigrp](#), on page 1265
- [ip load-sharing](#), on page 1267
- [ip network-broadcast](#), on page 1268
- [ip ospf database-filter all out](#), on page 1269
- [ip ospf name-lookup](#), on page 1270
- [ip split-horizon eigrp](#), on page 1271
- [ip summary-address eigrp](#), on page 1272
- [ip route static bfd](#), on page 1275
- [ipv6 route static bfd](#), on page 1277
- [metric weights \(EIGRP\)](#), on page 1279

- neighbor description, on page 1282
- network (EIGRP) , on page 1284
- nsf (EIGRP) , on page 1286
- offset-list (EIGRP) , on page 1288
- redistribute (IP) , on page 1290
- redistribute (IPv6) , on page 1299
- redistribute maximum-prefix (OSPF) , on page 1303
- route-map, on page 1305
- router-id, on page 1309
- router eigrp, on page 1310
- router ospfv3, on page 1311
- send-lifetime, on page 1312
- show ip eigrp interfaces, on page 1315
- show ip eigrp neighbors, on page 1318
- show ip eigrp topology, on page 1321
- show ip eigrp traffic, on page 1327
- show ip ospf, on page 1329
- show ip ospf border-routers, on page 1337
- show ip ospf database, on page 1338
- show ip ospf interface, on page 1348
- show ip ospf neighbor, on page 1352
- show ip ospf virtual-links, on page 1358
- summary-address (OSPF) , on page 1360
- timers throttle spf, on page 1362

accept-lifetime

キーチェーンの認証キーが有効なキーとして受信される期間を設定するには、**accept-lifetime** コマンドをキーチェーン キー コンフィギュレーション モードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
accept-lifetime [ local ] start-time { infinite end-time | duration seconds }
no accept-lifetime
```

Syntax Description		
	local	ローカルタイムゾーンで時刻を指定します。
	<i>start-time</i>	<p>key コマンドで指定したキーが受信できる開始時刻です。構文は次のいずれかにすることができます。</p> <p><i>hh</i> : <i>mm</i> : <i>ss</i> <i>month</i> <i>date</i> <i>year</i></p> <p><i>hh</i> : <i>mm</i> : <i>ss</i> <i>date</i> <i>month</i> <i>year</i></p> <ul style="list-style-type: none"> • <i>hh</i>: 時間 • <i>mm</i>: 分 • <i>ss</i>: 秒 • <i>month</i>: 月の最初の 3 文字 • <i>date</i>: 日 (1 ~ 31) • <i>year</i>: 年 (4 桁) <p>デフォルトの開始時刻で、指定できる最初の日付は 1993 年 1 月 1 日です。</p>
	infinite	キーは <i>start-time</i> 値以降、受信可能です。
	<i>end-time</i>	キーは、 <i>start-time</i> 値から <i>end-time</i> 値まで、受信可能です。シンタックスは <i>start-time</i> 値と同じです。 <i>end-time</i> は <i>start-time</i> 値の後である必要があります。デフォルトの終了時刻は無限の期間です。
	duration <i>seconds</i>	キーが受信可能な時間の長さ (秒単位) 指定できる範囲は 1 ~ 864000 です。

Command Default キーチェーン上の認証キーは、永久に有効として受信されます (開始時刻は 1993 年 1 月 1 日、終了時刻は無期限です)。

Command Modes キー チェーン キー コンフィギュレーション (config-keychain-key)

Command History リリース 変更内容

Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

Usage Guidelines

DRP エージェント、Enhanced Interior Gateway Routing Protocol (EIGRP)、および Routing Information Protocol (RIP) バージョン 2 のみがキーチェーンを使用します。

start-time 値と **infinite**、*end-time*、または **duration seconds** のいずれかの値を指定します。

キーにライフタイムを割り当てる場合は、Network Time Protocol (NTP) またはその他の時刻同期方式を実行することを推奨します。

最後のキーが期限切れになった場合、認証は続行されますが、エラーメッセージが生成されません。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

Examples

次の例では、**chain1** という名前のキーチェーンが設定されます。**key1** という名前のキーは午後 1 時 30 分から午後 3 時 30 分まで受け入れられ、午後 2 時 00 分から午後 3 時 00 分まで送信されます。**key2** という名前のキーは午後 2 時 30 分から午後 4 時 30 分まで受け入れられ、午後 3 時 00 分から午後 4 時 00 分まで送信されます。このオーバーラップにより、ルータの設定時間内でのキーの移行または不一致に対処できます。時間の違いを処理するために、前後に 30 分間の余裕が設けられています。

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# ip rip authentication key-chain chain1
Device(config-if)# ip rip authentication mode md5
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# network 172.19.0.0
Device(config-router)# version 2
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain)# key-string key2
Device(config-keychain)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

次に、**chain1** という名前のキーを EIGRP アドレスファミリに設定する例を示します。**Key1** という名前のキーは、午後 1 時 30 分から午後 3 時 30 分まで承認され、午後 2 時から午後 3 時まで送信されます。**Key2** という名前のキーは、午後 2 時 30 分から午後 4 時 30 分まで承認され、午後 3 時から午後 4 時まで送信されます。この重複により、キーの移行またはルータの設定時間の不一致に対処できます。時間の違いを処理するために、前後に 30 分間の余裕が設けられています。

```
Device(config)# router eigrp 10
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# authentication key-chain trees
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
```

```

Device(config-keychain-key) # accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key) # send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key) # exit
Device(config-keychain) # key 2
Device(config-keychain-key) # key-string key2
Device(config-keychain-key) # accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key) # send-lifetime 15:00:00 Jan 25 1996 duration 3600

```

Related Commands

Command	Description
key	キーチェーンの認証キーを識別します。
key chain	ルーティングプロトコルの認証をイネーブルにするために必要な認証キーチェーンを定義します。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

address-family ipv6 (OSPF)

標準の IPv6 アドレスプレフィックスを使用するルーティングセッション（Open Shortest Path First (OSPF) など）を設定するためにアドレス ファミリ コンフィギュレーション モードを開始するには、ルータ コンフィギュレーション モードで **address-family ipv6** コマンドを使用します。アドレス ファミリ コンフィギュレーション モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
address-family ipv6 [unicast ][vrf vrf-name ]
no address-family ipv6 [unicast ][vrf vrf-name ]
```

Syntax Description

unicast	(オプション) IPv6 ユニキャスト アドレス プレフィックスを指定します。
vrf	(オプション) IPv6 アドレスに対してすべての VPN ルーティングおよび転送 (VRF) インスタンステーブルまたは特定の VRF テーブルを指定します。
vrf-name	(オプション) IPv6 アドレスの特定の VRF テーブル。

Command Default

IPv6 アドレスプレフィックスはイネーブルではありません。IPv6 アドレスプレフィックスが設定されている場合は、ユニキャスト アドレス プレフィックスがデフォルトです。

Command Modes

ルータ コンフィギュレーション (config-router)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが した。

Usage Guidelines

address-family ipv6 コマンドは、ルータをアドレス ファミリ コンフィギュレーション モード（プロンプト: config-router-af）にします。このモードから、標準 IPv6 アドレスプレフィックスを使用するルーティングセッションを設定できます。

Examples

次の例は、ルータをアドレス ファミリ コンフィギュレーション モードに切り替える方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)#
```

Related Commands

コマンド	説明
router ospfv3	OSPFv3 ルータ コンフィギュレーション モードを開始します。

area nssa

Not-So-Stubby Area (NSSA) を設定するには、ルータアドレスファミリまたはルータ コンフィギュレーションモードで **area nssa** コマンドを使用します。エリアからNSSAの区別を削除するには、このコマンドの **no** 形式を使用します。

```
area nssa command area area-id nssa [no-redistribution] [default-information-originate [metric]
[metric-type]] [no-summary] [nssa-only]
no area area-id nssa [no-redistribution] [default-information-originate [metric] [metric-type]]
[no-summary] [nssa-only]
```

Syntax Description

<i>area-id</i>	スタブエリアまたはNSSAのID。IDは、10進数値またはIPアドレスで指定します。
no-redistribution	(任意) ルータがNSSAエリア境界ルータ (ABR) であり、 redistribute コマンドで、通常のエリアだけにルートをインポートし、NSSA エリアにインポートしない場合に使用します。
default-information-originate	(任意) タイプ7デフォルトをNSSAエリアに生成するために使用します。このキーワードは、NSSA ABR または NSSA 自律システム境界ルータ (ASBR) だけで有効です。
metric	(任意) OSPF デフォルト メトリックを指定します。
metric-type	(任意) デフォルト ルートの OSPF メトリック タイプを指定します。
no-summary	(任意) エリアをNSSAにすることを許可しますが、サマリー ルートを注入しません。
nssa-only	(任意) タイプ7LSAのPropagate (P) ビットを0に設定することで、このNSSAエリアに対するデフォルトアドバタイズメントを制限します。

Command Default

NSSA エリアは未定義です。

Command Modes

ルータアドレスファミリ トポロジ コンフィギュレーション (config-router-af-topology) ルータ コンフィギュレーション (config-router)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

指定したエリアをソフトウェア コンフィギュレーションから削除するには、**no area area-id** コマンドを使用します (他のキーワードは指定しません)。つまり、**no area area-id** コマンドは、**area authentication**、**area default-cost**、**area nssa**、**area range**、**area stub**、および **area virtual-link** などのすべてのエリアオプションを削除します。

Release 12.2(33)SRB

マルチトポロジルーティング（MTR）機能を使用する予定の場合は、この OSPF ルータ コンフィギュレーション コマンドをトポロジ対応にするために、ルータ アドレス ファミリ トポロジ コンフィギュレーション モードで **area nssa** コマンドを実行する必要があります。

Examples

次に、エリア 1 を NSSA エリアにする例を示します。

```
router ospf 1
 redistribute rip subnets
 network 172.19.92.0 0.0.0.255 area 1
 area 1 nssa
```

Related Commands

Command	Description
redistribute	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。

area virtual-link

Open Shortest Path First (OSPF) 仮想リンクを定義するには、ルータアドレスファミリトポロジ、ルータ コンフィギュレーション、またはアドレスファミリ コンフィギュレーションモードで **area virtual-link** コマンドを使用します。仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

```
area area-id virtual-link router-id authentication key-chain chain-name [hello-interval seconds]
[retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [ttl-security hops
hop-count]
```

```
no area area-id virtual-link router-id authentication key-chain chain-name
```

Syntax Description

Table 116:

<i>area-id</i>	仮想リンクに割り当てるエリア ID。10 進数値または有効な IPv6 プレフィックスを指定します。デフォルトはありません。
<i>router-id</i>	仮想リンク ネイバーに関連付けられるルータ ID。ルータ ID は show ip ospf または show ipv6 display コマンドで表示されます。デフォルトはありません。
authentication	仮想リンク認証を有効にします。
key-chain	暗号化認証キーのキーチェーンを設定します。
<i>chain-name</i>	有効な認証キーの名前。
hello-interval <i>seconds</i>	(任意) Cisco IOS ソフトウェアがインターフェイス上で送信する hello パケットの間隔 (秒単位) を指定します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数値です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセスサーバで同じである必要があります。有効な範囲は 1 ~ 8192 です。デフォルトは 10 です。
retransmit-interval <i>seconds</i>	(任意) インターフェイスに属する隣接に対するリンクステートアドバタイズメント (LSA) の再送信間隔 (秒単位) を指定します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延よりも大きい必要があります。有効な範囲は 1 ~ 8192 です。デフォルトは 5 分です。

transmit-delay <i>seconds</i>	(任意) インターフェイス上でリンクステートアップデートパケットを送信するために必要な推定される時間 (秒単位) を指定します。ゼロよりも大きい整数値を指定します。アップデートパケット内の LSA の経過時間は、転送前にこの値の分だけ増分されます。有効な範囲は 1 ~ 8192 です。デフォルト値は 1 です。
dead-interval <i>seconds</i>	(任意) hello パケットがどれだけの時間 (秒単位) 届かなかった場合にネイバーがルータをダウンと見なすかを指定します。デッドインターバルは符号なし整数値です。デフォルトは hello 間隔の 4 倍または 40 秒です。hello 間隔と同様に、この値は、共通のネットワークに接続されているすべてのルータとアクセスサーバで同じでなければなりません。
ttl-security hops <i>hop-count</i>	(任意) 仮想リンク上で存続可能時間 (TTL) セキュリティを設定します。引数 <i>hop-count</i> の範囲は 1 ~ 254 です。

Command Default OSPF 仮想リンクは定義されていません。

Command Modes ルータ アドレス ファミリ トポロジ コンフィギュレーション (config-router-af-topology)
 ルータ コンフィギュレーション (config-router)
 アドレス ファミリ コンフィギュレーション (config-router-af)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines OSPF では、すべてのエリアがバックボーンエリアに接続されている必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。

hello 間隔を短くするほど、トポロジの変更が速く検出されますが、ルーティングトラフィックの増加につながります。再送信間隔は控えめに設定する必要があります。そうしないと、不必要な再送信が発生します。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

インターフェイスの送信遅延と伝達遅延を考慮した伝送遅延値を選択する必要があります。

IPv6 の OSPF で仮想リンクを設定するには、アドレスではなくルータ ID を使用する必要があります。IPv6 の OSPF では、仮想リンクはリモートルータの IPv6 プレフィックスではなくルータ ID を使用します。

ネイバーからの OSPF パケット上の TTL 値のチェックをイネーブルにするか、ネイバーに送信される TTL 値を設定するには、**ttl-security hops hop-count** キーワードと引数を使用します。この機能により、OSPF にさらなる保護レイヤが追加されます。



Note 仮想リンクを正しく設定するには、各仮想リンク ネイバーにトランジット エリア ID と対応する仮想リンク ネイバー ルータ ID が設定されている必要があります。ルータ ID を表示するには、特権 EXEC モードで **show ip ospf** または **show ipv6 ospf** コマンドを使用します。



Note 指定したエリアをソフトウェア コンフィギュレーションから削除するには、**no area area-id** コマンドを使用します（他のキーワードは指定しません）。つまり、**no area area-id** コマンドは、**area default-cost**、**area nssa**、**area range**、**area stub**、および **area virtual-link** などのすべてのエリア オプションを削除します。

Release 12.2(33)SRB

マルチトポロジルーティング（MTR）機能を使用する予定の場合は、この OSPF ルータ コンフィギュレーション コマンドをトポロジ対応にするために、ルータ アドレス ファミリ トポロジ コンフィギュレーション モードで **area virtual-link** コマンドを実行する必要があります。

Examples

次に、すべてのオプション パラメータでデフォルト値を使用して、仮想リンクを確立する例を示します。

```
Device(config)# ipv6 router ospf 1
Device(config)# log-adjacency-changes
Device(config)# area 1 virtual-link 192.168.255.1
```

次に、IPv6 の OSPF で仮想リンクを確立する例を示します。

```
Device(config)# ipv6 router ospf 1
Device(config)# log-adjacency-changes
Device(config)# area 1 virtual-link 192.168.255.1 hello-interval 5
```

次の例に、IPv6 向けの OSPFv3 で仮想リンク用の TTL セキュリティを設定する方法を示します。

```
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast vrf vrf1
Device(config-router-af)# area 1 virtual-link 10.1.1.1 ttl-security hops 10
```

次の例に、仮想リンク用にキーチェーンを使用して認証を設定する方法を示します。

```
Device(config)# area 1 virtual-link 192.168.255.1 authentication key-chain ospf-chain-1
```

Related Commands

コマンド	説明
area	OSPFv3 エリア パラメータを設定します。
show ip ospf	OSPF ルーティングプロセスに関する全般的な情報の表示をイネーブルにします。
show ipv6 ospf	OSPF ルーティングプロセスに関する全般的な情報の表示をイネーブルにします。
ttl-security hops	ネイバーからの OSPF パケット上の TTL 値のチェックか、ネイバーに送信される TTL 値の設定をイネーブルにします。

authentication (BFD)

シングルホップセッション用の Bidirectional Forwarding Detection (BFD) テンプレートで認証を設定するには、BFD コンフィギュレーション モードで **authentication** コマンドを使用します。シングルホップセッション用の BFD テンプレートで認証を無効にするには、このコマンドの **no** 形式を使用します。

authentication *authentication-type* **keychain** *keychain-name*
no authentication *authentication-type* **keychain** *keychain-name*

Syntax Description

authentication-type 認証タイプ。有効な値は、md5、meticulous-md5、meticulous-sha1、および sha-1 です。

keychain *keychain-name* 指定された名前でも認証キーチェーンを設定します。この名前の長さは最大 32 文字です。

Command Default

シングルホップセッション用の BFD テンプレートでは認証が有効になっていません。

Command Modes

BFD コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

シングルホップテンプレートで認証を設定できます。セキュリティを強化するために認証を設定することをお勧めします。認証は、BFD の送信元と宛先のペアごとに設定する必要があり、認証パラメータは両方のデバイスで同じである必要があります。

Examples

次に、BFD シングルホップテンプレートの `template1` で認証を設定する例を示します。

```
Device>enable
Device#configuration terminal
Device(config)#bfd-template single-hop template1
Device(config-bfd)#authentication sha-1 keychain bfd-singlehop
```

bfd

インターフェイスに対してベースライン Bidirectional Forwarding Detection (BFD) セッションパラメータを設定するには、インターフェイス コンフィギュレーションモードで **bfd** コマンドを使用します。ベースライン BFD セッションパラメータを削除するには、このコマンドの **no** 形式を使用します。

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*
no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Syntax Description	interval	milliseconds
	BFD 制御パケットが BFD ピアに送信される速度（ミリ秒単位）を指定します。milliseconds 引数の有効範囲は 50 ～ 9999 です。	
	min_rx	<i>milliseconds</i>
	BFD 制御パケットが BFD ピアで受信されるものと期待される速度（ミリ秒単位）を指定します。milliseconds 引数の有効範囲は 50 ～ 9999 です。	
	multiplier	<i>multiplier-value</i>
	BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。multiplier-value 引数の有効範囲は 3 ～ 50 です。	

Command Default ベースライン BFD セッションパラメータの設定はありません。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines bfd コマンドは、SVI、イーサネット、およびポートチャネルインターフェイスで設定できます。BFD がポートチャネルインターフェイスで実行されている場合は、BFD には、750 * 3 ミリ秒のタイマー値制限があります。

bfd interval 設定は次のような場合には削除されません。

- IPv4 アドレスがインターフェイスから削除された場合
- IPv6 アドレスがインターフェイスから削除された場合
- IPv6 がインターフェイスからディセーブルにされた場合
- インターフェイスがシャットダウンされた場合
- インターフェイスで IPv4 CEF がグローバルまたはローカルでディセーブルにされた場合
- インターフェイスで IPv6 CEF がグローバルまたはローカルでディセーブルにされた場合

bfd interval 設定は、それを設定したサブインターフェイスが削除されたときに削除されます。



Note インターフェイス コンフィギュレーションモードで `bfd interval` コマンドを設定すると、デフォルトで BFD エコー モードが有効になります。インターフェイス コンフィギュレーションモードで `no ip redirect` (BFD エコーが必要な場合) または `no bfd echo` のいずれかを有効にする必要があります。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、`no ip redirect` コマンドを入力して、インターネット制御メッセージプロトコル (ICMP) リダイレクトメッセージの送信を無効にする必要があります。

Examples

次に、ギガビットイーサネット 1/0/3 の BFD セッションパラメータを設定する例を示します。

```
Device>enable
Device#configuration terminal
Device(config)#interface gigabitethernet 1/0/3
Device(config-if)#bfd interval 100 min_rx 100 multiplier 3
```

bfd all-interfaces

ルーティングプロセスに参加しているすべてのインターフェイスの Bidirectional Forwarding Detection (BFD) を有効にするには、ルータ コンフィギュレーション モードまたはアドレス ファミリ インターフェイス コンフィギュレーション モードで **bfd all-interfaces** コマンドを使用します。1 つのインターフェイスですべてのネイバーの BFD を無効にするには、このコマンドの **no** 形式を使用します。

bfd all-interfaces
no bfd all-interfaces

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

ルーティングプロセスに参加しているインターフェイスの BFD が無効になっています。

Command Modes

ルータ コンフィギュレーション (config-router)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

すべてのインターフェイスの BFD を有効にするには、ルータ コンフィギュレーション モードで **bfd all-interfaces** コマンドを入力します。

Examples

次に、すべての Enhanced Interior Gateway Routing Protocol (EIGRP) ネイバーの BFD を有効にする例を示します。

```
Device>enable
Device#configuration terminal
Device(config)#router eigrp 123
Device(config-router)#bfd all-interfaces
Device(config-router)#end
```

次に、すべての Intermediate System-to-Intermediate System (IS-IS) ネイバーの BFD を有効にする例を示します。

```
Device> enable
Device#configuration terminal
Device(config)#router isis tag1
Device(config-router)#bfd all-interfaces
Device(config-router)#end
```

bfd check-ctrl-plane-failure

Intermediate System-to-Intermediate System (IS-IS) ルーティングプロトコルの Bidirectional Forwarding Detection (BFD) コントロールプレーン障害チェックを有効にするには、ルータ コンフィギュレーション モードで **bfd check-control-plane-failure** コマンドを使用します。コントロールプレーン障害検出を無効にするには、このコマンドの **no** 形式を使用します。

bfd check-ctrl-plane-failure
no bfd check-ctrl-plane-failure

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

BFD コントロールプレーン障害チェックが無効になっています。

Command Modes

ルータ コンフィギュレーション (config-router)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

bfd check-ctrl-plane-failure コマンドは、IS-IS ルーティングプロセスについてのみ設定できます。このコマンドは、他のプロトコルではサポートされていません。

スイッチが再起動すると、見せかけの BFD セッション障害が発生する場合があります。このとき、隣接ルータは、転送障害が本当に発生したかのように動作します。ただし、スイッチで **bfd check-control-plane-failure** コマンドが有効になっていると、ルータはコントロールプレーン関連の BFD セッション障害を無視できます。ルータを再起動する予定がある場合は、直前にすべての隣接ルータの設定にこのコマンドを追加し、再起動が完了したときにすべての隣接ルータからこのコマンドを削除することをお勧めします。

Examples

次に、IS-IS ルーティングプロトコルの BFD コントロールプレーン障害チェックを有効にする例を示します。

```
Device>enable
Device#configuration terminal
Device(config)#router isis
Device(config-router)#bfd check-ctrl-plane-failure
Device(config-router)#end
```

bfd echo

Bidirectional Forwarding Detection (BFD) エコーモードを有効にするには、インターフェイス コンフィギュレーションモードで **bfd echo** コマンドを使用します。BFD エコーモードを無効にするには、このコマンドの **no** 形式を使用します。

bfd echo
no bfd echo

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default インターフェイス コンフィギュレーションモードで **bfd interval** コマンドを使用して BFD を設定している場合は、BFD エコーモードがデフォルトで有効になります。

Command Modes インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines エコーモードはデフォルトでイネーブルになっています。キーワードを指定せずに **no bfd echo** コマンドを入力すると、エコーパケットの送信がオフになり、スイッチが BFD ネイバースイッチから受信したエコーパケットを転送しないことを示します。

エコーモードを有効にすると、必要最短エコー送信間隔と必要最短送信間隔の値が **bfd interval milliseconds min_rx milliseconds** パラメータから取得されます。



Note CPU 使用率の上昇を避けるために、BFD エコーモードを使用する前に、**no ip redirects** コマンドを入力して、インターネット制御メッセージプロトコル (ICMP) リダイレクトメッセージの送信を無効にする必要があります。

Examples

次に、BFD ネイバー間でエコーモードを設定する例を示します。

```
Device>enable
Device#configuration terminal
Device(config)#interface GigabitEthernet 1/0/3
Device(config-if)#bfd echo
```

show bfd neighbors details コマンドの次の出力は、BFD セッションネイバーが BFD エコーモードで稼働しているところを示します。この出力では、対応するコマンド出力が太字で表示されています。

```
Device#show bfd neighbors details
OurAddr      NeighAddr  LD/RD  RH/RS  Holdown(mult)  State  Int
172.16.1.2   172.16.1.1  1/6    Up      0 (3 )         Up     Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1          - Diagnostic: 0
              State bit: Up      - Demand bit: 0
              Poll bit: 0        - Final bit: 0
              Multiplier: 3      - Length: 24
              My Discr.: 6       - Your Discr.: 1
              Min tx interval: 1000000 - Min rx interval: 1000000
              Min Echo interval: 50000
```

bfd slow-timers

Bidirectional Forwarding Detection (BFD) スロータイマー値を設定するには、インターフェイス コンフィギュレーション モードで **bfd slow-timers** コマンドを使用します。BFD によって使用されるスロータイマーを変更するには、このコマンドの **no** 形式を使用します。

bfd slow-timers [*milliseconds*]
no bfd slow-timers

Command Default BFD スロータイマー値は 1000 ミリ秒です。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、BFD スロータイマー値を 14,000 ミリ秒に設定する例を示します。

```
Device(config)#bfd slow-timers 14000
```

show bfd neighbors details コマンドの次の出力は、BFD スロータイマー値 14,000 ミリ秒が実装されているところを示します。MinTxInt および MinRxInt の値は BFD スロータイマーの設定値に対応しています。関連するコマンド出力は太字で示されています。

```
Device#show bfd neighbors details
OurAddr      NeighAddr  LD/RD  RH/RS  Holdown(mult)  State  Int
172.16.1.2   172.16.1.1  1/6    Up      0 (3)          Up     Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 14000, MinRxInt: 14000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1           - Diagnostic: 0
                State bit: Up       - Demand bit: 0
                Poll bit: 0         - Final bit: 0
                Multiplier: 3       - Length: 24
                My Discr.: 6        - Your Discr.: 1
                Min tx interval: 1000000 - Min rx interval: 1000000
                Min Echo interval: 50000
```

**Note**

- BFDセッションがダウンすると、BFD制御パケットがスロータイマー間隔で送信されます。
- BFDセッションが稼働している場合、エコーが有効になっていれば、BFD制御パケットがネゴシエートされたスロータイマー間隔で送信され、エコーパケットがネゴシエートされた設定済みのBFD間隔で送信されます。エコーが有効になっていない場合は、BFD制御パケットがネゴシエートされた設定済みの間隔で送信されます。

bfd template

Bidirectional Forwarding Detection (BFD) テンプレートを設定し、BFD コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **bfd-template** コマンドを使用します。BFD テンプレートを削除するには、このコマンドの **no** 形式を使用します。

```
bfd template template-name  
no bfd template template-name
```

Command Default BFD テンプレートはインターフェイスにバインドされません。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **bfd-template** コマンドを使用してテンプレートを作成していない場合でも、インターフェイスでテンプレート名を設定できますが、テンプレートを定義するまでテンプレートは無効と見なされます。テンプレート名を再設定する必要はありません。名前は自動的に有効になります。

Examples

```
Device> enable  
Device#configuration terminal  
Device(config)#interface GigabitEthernet 1/3/0  
Device(config-if)#bfd template template1
```

bfd-template single-hop

シングルホップ Bidirectional Forwarding Detection (BFD) テンプレートをインターフェイスにバインドするには、インターフェイス コンフィギュレーション モードで **bfd template** コマンドを使用します。シングルホップ BFD テンプレートをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

bfd-template single-hop *template-name*
no bfd-template single-hop *template-name*

Syntax Description

single-hop シングルホップ BFD テンプレートを作成します。

template-name テンプレート名。

Command Default

BFD テンプレートは存在しません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
------	------

Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
--------------------------	-----------------

Usage Guidelines

bfd template コマンドを使用すると BFD テンプレートを作成し、デバイスを BFD コンフィギュレーションモードにすることができます。テンプレートは一連の BFD 間隔値を指定するために使用できます。BFD テンプレートの一部として指定される BFD 間隔値は、1つのインターフェイスに限定されるものではありません。

Examples

次に、BFD テンプレートを作成し、BFD 間隔値を指定する例を示します。

```
Device>enable
Device#configuration terminal
Device(config)#bfd-template single-hop node1
Device(bfd-config)#interval min-tx 100 min-rx 100 multiplier 3
Device(bfd-config)#echo
```

次に、BFD シングルホップテンプレートを作成し、BFD 間隔値と認証キー チェーンを設定する例を示します。

```
Device> enable
Device#configuration terminal
Device(config)#bfd-template single-hop template1
Device(bfd-config)#interval min-tx 200 min-rx 200 multiplier 3
Device(bfd-config)#authentication keyed-sha-1 keychain bfd_singlehop
```



Note デフォルトでは、BFD テンプレート設定で BFD エコーは有効になっていません。これは明示的に設定する必要があります。

default-information originate (OSPF)

デフォルト外部ルートを Open Shortest Path First (OSPF) ルーティングドメイン内に生成するには、ルータ コンフィギュレーション モードまたはルータ アドレス ファミリ トポロジ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]

Syntax Description

always	(任意) ソフトウェアにデフォルト ルートがあるかどうかにかかわらず、常に、デフォルト ルートをアドバタイズします。 Note ルートマップを使用する場合、キーワード always には次の例外が含まれます。ルートマップを使用する場合、OSPF によるデフォルト ルートの送信は、ルーティングテーブル内にデフォルト ルートが存在するかどうかによって制限されず、 always キーワードは無視されます。
metric <i>metric-value</i>	(任意) デフォルト ルートを生成するために使用するメトリック。値を省略して、 default-metric ルータ コンフィギュレーション コマンドを使用して値を指定しない場合、デフォルトのメトリック値は10になります。使用される値はプロトコル固有です。
metric-type <i>type-value</i>	(任意) OSPF ルーティング ドメインにアドバタイズされる、デフォルト ルートに関連付けられた外部リンク タイプ次のいずれかの値を指定できます。 <ul style="list-style-type: none"> • タイプ 1 外部ルート。 • タイプ 2 外部ルート。 デフォルトはタイプ 2 外部ルートです。
route-map <i>map-name</i>	(任意) ルーティングプロセスは、ルートマップが満たされている場合にデフォルト ルートを生成します。

Command Default

このコマンドは、デフォルトでディセーブルになっています。OSPF ルーティング ドメイン内にデフォルト外部ルートは生成されません。

Command Modes

ルータ コンフィギュレーション (config-router) ルータ アドレス ファミリ トポロジ コンフィギュレーション (config-router-af-topology)

Command History

Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
--------------------------	-----------------

Usage Guidelines

redistribute または **default-information** ルータ コンフィギュレーション コマンドを使用して、OSPF ルーティング ドメイン にルート を再配布する場合、Cisco IOS ソフトウェア は自動的に自律システム境界ルータ (ASBR) になります。ただし、デフォルトでは、ASBR はデフォルトルートを OSPF ルーティング ドメイン に生成しません。キーワード **always** を指定した場合を除き、ソフトウェア には、デフォルトルートを生成する前に、自身のためにデフォルトルートが設定されている必要 があります。

ルート マップを使用する場合、OSPF によるデフォルトルートの送信は、ルーティング テーブル 内にデフォルト ルートが存在するかどうかによって制限されません。

Release 12.2(33)SRB

マルチトポロジルーティング (MTR) 機能を使用する予定の場合は、この OSPF ルータ コンフィギュレーション コマンドをトポロジ対応にするために、ルータ アドレス ファミリ トポロジ コンフィギュレーション モードで **default-information originate** コマンドを実行する必要があります。

Examples

次に、OSPF ルーティング ドメイン に再配布されるデフォルトルートのメトリックを 100 に指定し、外部メトリック タイプをタイプ 1 に指定する例を示します。

```
router ospf 109
 redistribute eigrp 108 metric 100 subnets
 default-information originate metric 100 metric-type 1
```

Related Commands

Command	Description
default-information	Enhanced Interior Gateway Routing Protocol (EIGRP) プロセスに外部情報またはデフォルト情報を受け入れます。
default-metric	ルートのデフォルトメトリック値を設定します。
redistribute (IP)	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。

distance (OSPF)

アドミニストレーティブ ディスタンスを定義するには、ルータ コンフィギュレーション モードまたは VRF コンフィギュレーション モードで **distance** コマンドを使用します。 **distance** コマンドを削除し、システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

distance *weight*

[*ip-address wildcard-mask* [*access-list name*]]

no distance *weight ip-address wildcard-mask* [*access-list-name*]

Syntax Description

<i>weight</i>	アドミニストレーティブ ディスタンス。範囲は 10 ~ 255 です。単独で使用される場合、 <i>weight</i> 引数は、ルーティング情報ソースに他の指定がない場合にソフトウェアが使用するデフォルトのアドミニストレーティブ ディスタンスを指定します。アドミニストレーティブ ディスタンスが 255 のルートはルーティングテーブルに格納されません。「使用上のガイドライン」の項の表に、デフォルトのアドミニストレーティブ ディスタンスがリストされています。
<i>ip-address</i>	(任意) 4 分割ドット付き 10 進表記の IP アドレス。
<i>wildcard-mask</i>	(任意) 4 分割ドット付き 10 進表記のワイルドカード マスク。 <i>wildcard-mask</i> 引数でビットが 1 に設定されている場合、ソフトウェアは、アドレス値で対応するビットを無視します。
<i>access-list-name</i>	(任意) 着信ルーティング アップデートに適用される IP アクセス リストの名前。

Command Default

このコマンドが指定されていない場合、アドミニストレーティブ ディスタンスはデフォルトになります。「使用上のガイドライン」の項の表に、デフォルトのアドミニストレーティブ ディスタンスがリストされています。

Command Modes

ルータ コンフィギュレーション (config-router)

VRF コンフィギュレーション (config-vrf)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザグループに属している必要があります。ユーザグループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

アドミニストレーティブ ディスタンスは、10 ~ 255 の整数です。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブ ディスタンスは、ルーティング情報源

がまったく信頼できないため、無視すべきであることを意味します。重み値は主観的に選択します。重み値を選択するための定量的方法はありません。

アクセスリストがこのコマンドで使用される場合、ネットワークがルーティングテーブルに挿入されるときに適用されます。この動作により、ルーティング情報を提供する IP プレフィックスに基づいてネットワークをフィルタリングできます。たとえば、管理制御下でないネットワークングデバイスからの、間違っている可能性があるルーティング情報をフィルタリングできます。

distance コマンドを実行する順序は、「例」の項に示すように、割り当てられるアドミニストレーティブディスタンスに影響を与える可能性があります。次の表に、デフォルトのアドミニストレーティブディスタンスを示します。

Table 117: デフォルトのアドミニストレーティブディスタンス

レート ソース	デフォルト距離
接続されているインターフェイス	0
インターフェイスからのスタティック ルート	0
ネクスト ホップへのスタティック ルート	1
EIGRP 集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP バージョン 1 および 2	120
外部 EIGRP	170
内部 BGP	200
不明	255

タスク ID

タスク ID	動作
ospf	読み取り、書き込み

Examples

次の例では、**router ospf** コマンドを使用して、Open Shortest Path First (OSPF) ルーティングインスタンス 1 を設定しています。最初の **distance** コマンドは、デフォルトのアドミニストレーティブディスタンスを 255 に設定します。つまり、ソフトウェアは、明示的なディスタンスが設定されていないネットワークングデバイスからのすべてのルーティン

グアプデートを無視します。2番目の **distance** コマンドは、ネットワーク 192.168.40.0 上のすべてのデバイスのアドミニストレーティブディスタンスを 90 に設定します。

```
Device#configure terminal
Device(config)#router ospf 1
Device(config-ospf)#distance 255
Device(config-ospf)#distance 90 192.168.40.0 0.0.0.255
```

Related Commands

コマンド	説明
distance bgp	BGP ノードへの最適なルートである可能性がある、外部、内部およびローカルアドミニストレーティブディスタンスの使用を許可します。
distance ospf	OSPF ノードへの最適なルートである可能性がある、外部、内部およびローカルアドミニストレーティブディスタンスの使用を許可します。
router ospf	OSPF ルーティングプロセスを設定します。

eigrp log-neighbor-changes

Enhanced Interior Gateway Routing Protocol (EIGRP) 隣接関係の変更のロギングをイネーブルにするには、ルータ コンフィギュレーションモード、アドレスファミリ コンフィギュレーションモード、またはサービスファミリ コンフィギュレーションモードで **eigrp log-neighbor-changes** コマンドを使用します。EIGRP 隣接関係の変化に関するロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-changes
no eigrp log-neighbor-changes

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default 隣接関係の変更がロギングされます。

Command Modes ルータ コンフィギュレーション (config-router) アドレス ファミリ コンフィギュレーション (config-router-af) サービス ファミリ コンフィギュレーション (config-router-sf)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、ルーティングシステムの安定性を監視して問題の検出に役立てるために、ネイバー ルータとの隣接関係の変更のロギングをイネーブルにします。デフォルトでは、ロギングはイネーブルです。隣接関係の変更のロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

EIGRP アドレスファミリ隣接関係の変更のロギングをイネーブルにするには、アドレスファミリ コンフィギュレーションモードで **eigrp log-neighbor-changes** コマンドを使用します。

EIGRP サービスファミリ隣接関係の変更のロギングをイネーブルにするには、サービスファミリ コンフィギュレーションモードで **eigrp log-neighbor-changes** コマンドを使用します。

Examples

次の設定は、EIGRP プロセス 209 について隣接関係の変更のロギングをディセーブルにします。

```
Device(config)# router eigrp 209
Device(config-router)# no eigrp log-neighbor-changes
```

次の設定は、EIGRP プロセス 209 について隣接関係の変更のロギングをイネーブルにします。

```
Device(config)# router eigrp 209
Device(config-router)# eigrp log-neighbor-changes
```

次に、自律システム 4453 で EIGRP アドレスファミリの隣接の変更のロギングをディセーブルにする例を示します。

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# no eigrp log-neighbor-changes
Device(config-router-af)# exit-address-family
```

次の設定は、EIGRP サービス ファミリ プロセス 209 について隣接関係の変更のロギングをイネーブルにします。

```
Device(config)# router eigrp 209
Device(config-router)# service-family ipv4 autonomous-system 4453
Device(config-router-sf)# eigrp log-neighbor-changes
Device(config-router-sf)# exit-service-family
```

Related Commands

コマンド	説明
address-family (EIGRP)	アドレスファミリ コンフィギュレーションモードを開始して、EIGRP ルーティング インスタンスを設定します。
exit-address-family	アドレス ファミリ コンフィギュレーション モードを終了します。
exit-service-family	サービス ファミリ コンフィギュレーション モードを終了します。
router eigrp	EIGRP ルーティング プロセスを設定します。
service-family	サービス ファミリ コンフィギュレーション モードを指定します。

eigrp log-neighbor-warnings

Enhanced Interior Gateway Routing Protocol (EIGRP) ネイバー警告メッセージのロギングを有効にするには、ルータ コンフィギュレーション モード、アドレスファミリ コンフィギュレーション モード、またはサービスファミリ コンフィギュレーション モードで **eigrp log-neighbor-warnings** コマンドを使用します。EIGRP ネイバー警告メッセージのロギングを無効にするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-warnings [*seconds*]
no eigrp log-neighbor-warnings

Syntax Description	<i>seconds</i>	(任意) ネイバー警告メッセージの反復間隔 (秒数)。有効な範囲は 1 ~ 65535 です。デフォルトは 10 です。
---------------------------	----------------	--

Command Default ネイバー警告メッセージが 10 秒間隔でログに記録されます。

Command Modes ルータ コンフィギュレーション (config-router) アドレス ファミリ コンフィギュレーション (config-router-af) サービス ファミリ コンフィギュレーション (config-router-sf)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ネイバー警告メッセージが発生すると、デフォルトでログに記録されます。このコマンドを使用すると、ネイバー警告メッセージを無効および有効にしたり、ネイバー警告メッセージの反復間隔を設定したりすることができます。

EIGRP アドレスファミリの警告メッセージのロギングを有効にするには、アドレスファミリ コンフィギュレーション モードで **eigrp log-neighbor-warnings** コマンドを使用します。

EIGRP サービスファミリの警告メッセージのロギングを有効にするには、サービスファミリ コンフィギュレーション モードで **eigrp log-neighbor-warnings** コマンドを使用します。

Examples

次のコマンドでは、EIGRP プロセス 209 のネイバー警告メッセージがログに記録され、5 分 (300 秒) 間隔で警告メッセージが繰り返されます。

```
Device(config)# router eigrp 209
Device(config-router)# eigrp log-neighbor-warnings 300
```

次に、自律システム番号 4453 のサービスファミリのネイバー警告メッセージをログに記録し、5 分 (300 秒) 間隔で警告メッセージを繰り返す例を示します。

```
Device(config)# router eigrp virtual-name
Device(config-router)# service-family ipv4 autonomous-system 4453
Device(config-router-sf)# eigrp log-neighbor-warnings 300
```

次に、自律システム番号 4453 のアドレスファミリのネイバー警告メッセージをログに記録し、5 分（300 秒）間隔で警告メッセージを繰り返す例を示します。

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# eigrp log-neighbor-warnings 300
```

Related Commands

コマンド	説明
address-family (EIGRP)	アドレスファミリ コンフィギュレーションモードを開始して、EIGRP ルーティング インスタンスを設定します。
exit-address-family	アドレス ファミリ コンフィギュレーション モードを終了します。
exit-service-family	サービス ファミリ コンフィギュレーション モードを終了します。
router eigrp	EIGRP ルーティング プロセスを設定します。
service-family	サービス ファミリ コンフィギュレーション モードを指定します。

ip authentication key-chain eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) パケットの認証を有効にするには、インターフェイス コンフィギュレーション モードで **ip authentication key-chain eigrp** コマンドを使用します。このような認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip authentication key-chain eigrp *as-number* *key-chain*
no ip authentication key-chain eigrp *as-number* *key-chain*

Syntax Description

<i>as-number</i>	認証が適用される自律システム番号
<i>key-chain</i>	認証キー チェーン名

Command Default

EIGRP パケットには認証は適用されません。

Command Modes

インターフェイス コンフィギュレーション (config-if) 仮想ネットワーク インターフェイス (config-if-vnet)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、自律システム 2 に認証を適用し、SPORTS というキー チェーン名を識別する例を示します。

```
Device(config-if)#ip authentication key-chain eigrp 2 SPORTS
```

Related Commands

Command	Description
accept-lifetime	キー チェーンの認証キーが有効として受信される期間を設定します。
ip authentication mode eigrp	EIGRP パケットで使用される認証タイプを指定します。
key	キー チェーンの認証キーを識別します。
key chain	ルーティング プロトコルの認証をイネーブルにします。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キー チェーンの認証キーが有効に送信される期間を設定します。

ip authentication mode eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) パケットに使用される認証タイプを指定するには、インターフェイス コンフィギュレーション モードで **ip authentication mode eigrp** コマンドを使用します。認証タイプをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip authentication mode eigrp as-number md5
no ip authentication mode eigrp as-number md5

Syntax Description	
<i>as-number</i>	自律システム (AS) 番号。
md5	キー付き Message Digest 5 (MD5) 認証。

Command Default EIGRP パケットには認証は適用されません。

Command Modes インターフェイス コンフィギュレーション (config-if) 仮想ネットワーク インターフェイス (config-if-vnet)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 認証を設定して、未承認のソースによる無許可または不正なルーティング メッセージの導入を防ぎます。認証が設定される際に、MD5 キー付きダイジェストが指定された自律システム内の各 EIGRP パケットに追加されます。

Examples

次に、自律システム 10 にある EIGRP パケットで MD5 認証を使用するためにインターフェイスを設定する例を示します。

```
Device(config-if)#ip authentication mode eigrp 10 md5
```

Related Commands	Command	Description
	accept-lifetime	キー チェーンの認証キーが有効として受信される期間を設定します。
	ip authentication key-chain eigrp	EIGRP パケットの認証をイネーブルにします。
	key	キー チェーンの認証キーを識別します。
	key chain	ルーティング プロトコルの認証をイネーブルにします。
	key-string (authentication)	キーの認証文字列を指定します。

Command	Description
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。

ip bandwidth-percent eigrp

インターフェイス上で Enhanced Interior Gateway Routing Protocol (EIGRP) で使用される可能性ある帯域幅の割合を設定するには、インターフェイス コンフィギュレーション モードで **ip bandwidth-percent eigrp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip bandwidth-percent eigrp *as-number percent*
no ip bandwidth-percent eigrp *as-number percent*

Syntax Description

<i>as-number</i>	自律システム (AS) 番号。
<i>percent</i>	EIGRP で使用できる帯域幅のパーセント

Command Default

EIGRP では、利用可能な帯域幅の 50% を使用できます。

Command Modes

インターフェイス コンフィギュレーション (config-if) 仮想ネットワーク インターフェイス (config-if-vnet)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

bandwidth インターフェイス コンフィギュレーション コマンドで定義されているように、EIGRP はリンクの帯域幅を 50% まで使用します。このコマンドは、帯域幅のその他のフラクションが必要な場合に使用できます。100% を超える値が設定されている可能性があることに注意してください。他の理由で帯域幅が意図的に低く設定されている場合、この設定オプションは便利な場合があります。

Examples

次に、EIGRP で、自律システム 209 の 56-kbps シリアルリンクを最大 75% (42 kbps) 使用できるようにする例を示します。

```
Device(config)#interface serial 0
Device(config-if)#bandwidth 56
Device(config-if)#ip bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
bandwidth (interface)	インターフェイスの帯域幅値を設定します。

ip cef load-sharing algorithm

Cisco Express Forwarding ロードバランシング アルゴリズムを選択するには、グローバル コンフィギュレーション モードで **ip cef load-sharing algorithm** コマンドを使用します。デフォルトのユニバーサル ロードバランシング アルゴリズムに戻るには、このコマンドの **no** 形式を使用します。

ip cef load-sharing algorithm {**original** | [**universal** [*id*]]}
no ip cef load-sharing algorithm

Syntax Description

original	送信元および宛先のハッシュに基づいて、ロードバランス アルゴリズムを元のアルゴリズムに設定します。
universal	送信元ハッシュ、宛先ハッシュ、ID ハッシュを使用するユニバーサル アルゴリズムに、ロードバランシング アルゴリズムを設定します。
<i>id</i>	(任意) 固定 ID。

Command Default

ユニバーサルロードバランシングアルゴリズムがデフォルトで選択されています。ロードバランシング アルゴリズムに固定識別子を設定しなかった場合、ルータは固有 ID を自動的に生成します。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

Cisco Express Forwarding のオリジナルのロードバランシング アルゴリズムでは、すべてのデバイスで同じアルゴリズムが使用されるため、複数のデバイスにわたるロードシェアリングで歪みが発生していました。ロードバランシング アルゴリズムをユニバーサルモードに設定すると、ネットワークのそれぞれのデバイスは、送信元アドレスと宛先アドレスのペアごとに別々のロードシェアリング決定を下すことができるようになり、ロードバランシングのゆがみが解消します。

Examples

次に、Cisco Express Forwarding の元のロードバランシング アルゴリズムを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip cef load-sharing algorithm original
Device(config)# exit
```

Related Commands

コマンド	説明
ip load-sharing	シスコ エクスプレス フォワーディングのロードバランシングをイネーブルにします。

ip prefix-list

プレフィックスリストを作成したり、プレフィックスリストエントリを追加するには、グローバルコンフィギュレーションモードで **ip prefix-list** コマンドを使用します。プレフィックスリストエントリを削除するには、このコマンドの **no** 形式を使用します。

ip prefix-list {*list-name* [*seq number*] {**deny**|**permit**} *network/length* [**ge** *ge-length*] [**le** *le-length*] | **description** 説明 | **sequence-number**}

no ip prefix-list {*list-name* [*seq number*] [{**deny**|**permit**} *network/length* [**ge** *ge-length*] [**le** *le-length*]] | **description** 説明 | **sequence-number**}

Syntax Description

<i>list-name</i>	プレフィックスリストを識別するための名前を設定します。「detail」または「summary」という単語は、 show ip prefix-list コマンドのキーワードであるため、リスト名として使用しないでください。
seq	(任意) プレフィックスリストエントリにシーケンス番号を適用します。
<i>number</i>	(任意) 1 ~ 4294967294 の整数。このコマンドを設定するときにシーケンス番号が入力されない場合は、デフォルトのシーケンス番号がプレフィックスリストに適用されます。最初のプレフィックスエントリに番号 5 が適用され、後続の番号のないエントリには 5 ずつ増えた番号が適用されます。
deny	一致した条件へのアクセスを拒否します。
permit	一致した条件へのアクセスを許可します。
<i>network / length</i>	ネットワークアドレスおよびネットワークマスクの長さ (ビット単位) を設定します。ネットワーク番号には、任意の有効な IP アドレスまたはプレフィックスを指定できます。ビットマスクは 1 から 32 までの番号を使用できます。
ge	(任意) 引数 <i>ge-length</i> を指定された範囲に適用することにより、範囲の下限 (範囲の説明の「~から」の部分) を指定します。 Note ge キーワードは、演算子の「以上」を表します。
<i>ge-length</i>	(任意) 照合されるプレフィックスの最小の長さを表します。
le	(任意) 引数 <i>le-length</i> を指定された範囲に適用することにより、範囲の上限 (範囲の説明の「~まで」の部分) を指定します。 Note le キーワードは、演算子の「以下」を表します。
<i>le-length</i>	(任意) 照合されるプレフィックスの最大の長さを表します。
description	(任意) プレフィックスリストに記述名を設定します。
<i>description</i>	(任意) プレフィックスリストの記述名 (1 ~ 80 文字の長さ)。

sequence-number	(任意) プレフィックス リストのシーケンス番号の使用を有効または無効にします。
------------------------	--

Command Default プレフィックス リストまたはプレフィックスリスト エントリは作成されません。

Command Modes グローバル コンフィギュレーション (config)

Command History *Table 118:*

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IP プレフィックス フィルタリングを設定するには、**ip prefix-list** コマンドを使用します。一致条件に基づいてプレフィックスを許可または拒否するには、プレフィックスリストを **permit** または **deny** キーワードを指定して設定します。どのプレフィックスリストのエントリとも一致しないトラフィックに暗黙拒否が適用されます。

プレフィックスリスト エントリは、IP アドレスとビット マスクで構成されています。IP アドレスは、クラスフルなネットワーク、サブネット、または単一のホストルート用にできます。ビット マスクは、1 ~ 32 の数値です。

プレフィックスリストは、完全なプレフィックス長の一致、または **ge** キーワードと **le** キーワードが使用されている場合は範囲内の一致に基づいてトラフィックをフィルタリングするように設定されます。**ge** キーワードと **le** キーワードは、プレフィックス長の範囲を指定するために使用され、*networklength* 引数だけを使用するよりも柔軟な設定を提供します。プレフィックスリストは、**ge** キーワードと **le** キーワードのどちらも指定されていない場合、完全一致を使用して処理されます。**ge** 値のみが指定されている場合、範囲は **ge ge-length** 引数に入力された値から完全な 32 ビットの長さまでです。**le** 値のみが指定されている場合、範囲は *networklength* 引数に入力された値から **le le-length** 引数までです。**ge ge-length** と **le le-length** の両方のキーワードと引数が入力された場合、その範囲は *ge-length* 引数と *le-length* 引数に使用される値の間です。

この動作は、次の式で表すことができます。

$length < ge\ ge-length < le\ le-length \leq 32$

シーケンス番号なしで **seq** キーワードが設定されている場合、デフォルトのシーケンス番号は 5 です。このシナリオでは、最初のプレフィックスリスト エントリには番号 5 が割り当てられ、後続のプレフィックスリスト エントリは 5 ずつ増分します。たとえば、次の 2 つのエントリはシーケンス番号 10 と 15 を持ちます。最初のプレフィックス リスト エントリにシーケンス番号が入力され、後続のエントリには入力されない場合、後続のエントリ番号は 5 ずつ増分します。たとえば、最初に設定されたシーケンス番号が 3 の場合、後続のエントリは 8、13、および 18 になります。デフォルトのシーケンス番号を抑制するには、**seq** キーワードを指定して **no ip prefix-list** コマンドを入力します。

プレフィックス リストの評価はシーケンス番号が最も小さいものから開始し、一致するものが見つかるまで順番に評価していきます。IP アドレスの一致が見つかったら、そのネットワークに permit または deny 文が適用され、リストの残りは評価されません。



Tip 最も処理される頻度の高いプレフィックスリスト文のシーケンス番号を最小にすれば、最良のパフォーマンスを得ることができます。seq number キーワードと引数はリシーケンスに使用できません。

neighbor prefix-list コマンドを入力すると、特定のピアのインバウンドまたはアウトバウンドアップデートにプレフィックスリストが適用されます。プレフィックスリストの情報とカウンタは、**show ip prefix-list** コマンドの出力に表示されます。prefix-list カウンタをリセットするには、**clear ip prefix-list** コマンドを入力します。

Examples

次の例では、プレフィックスリストがデフォルトルート 0.0.0.0/0 を拒否するように設定されています。

```
Device(config)#ip prefix-list RED deny 0.0.0.0/0
```

次の例では、プレフィックスリストが 172.16.1.0/24 サブネットからのトラフィックを許可するように設定されています。

```
Device(config)#ip prefix-list BLUE permit 172.16.1.0/24
```

次の例では、プレフィックスリストが 24 ビット以下のマスク長を持つ 10.0.0.0/8 ネットワークからのルートを許可するように設定されています。

```
Device(config)#ip prefix-list YELLOW permit 10.0.0.0/8 le 24
```

次の例では、プレフィックスリストが 25 ビット以上のマスク長を持つ 10.0.0.0/8 ネットワークからのルートを拒否するように設定されています。

```
Device(config)#ip prefix-list PINK deny 10.0.0.0/8 ge 25
```

次の例では、マスク長が 8 ~ 24 ビットの任意のネットワークからのルートを許可するようにプレフィックスリストが設定されています。

```
Device(config)#ip prefix-list GREEN permit 0.0.0.0/0 ge 8 le 24
```

次の例では、プレフィックスリストが 10.0.0.0/8 ネットワークからの任意のマスク長を持つルートを拒否するように設定されています。

```
Device(config)#ip prefix-list ORANGE deny 10.0.0.0/8 le 32
```

Related Commands

コマンド	説明
clear ip prefix-list	プレフィックスリストのエントリカウンタをリセットします。
ip prefix-list description	プレフィックスリストのテキスト説明を追加します。

コマンド	説明
ip prefix-list sequence	デフォルトのプレフィックスリストシーケンシングを有効または無効にします。
match ip address	標準アクセスリストまたは拡張アクセスリストで許可された宛先ネットワーク番号アドレスを含むすべてのルートを配布し、パケットに対してポリシールーティングを実行します。
neighbor prefix-list	プレフィックスリストを使用して、指定されたネイバーからのルートをフィルタリングします。
show ip prefix-list	プレフィックスリストまたはプレフィックスリストエントリに関する情報を表示します。

ip hello-interval eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) プロセスの Hello インターバルを設定するには、インターフェイス コンフィギュレーション モードで **ip hello-interval eigrp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip hello-interval eigrp *as-number seconds*
no ip hello-interval eigrp *as-number [seconds]*

Syntax Description	
<i>as-number</i>	自律システム (AS) 番号。
<i>seconds</i>	hello インターバル (秒単位)。有効な範囲は 1 ~ 65535 です。

Command Default 低速の非ブロードキャスト マルチアクセス (NBMA) ネットワークの hello インターバルは 60 秒で、その他のすべてのネットワークは 5 秒です。

Command Modes インターフェイス コンフィギュレーション (config-if) 仮想ネットワーク インターフェイス (config-if-vnet)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デフォルトの 60 秒は、低速の NBMA メディアだけに適用されます。低速とは、**bandwidth** インターフェイス コンフィギュレーション コマンドで指定されているように、T1 以下のレートのことを指します。EIGRP、フレーム リレー、およびスイッチド マルチメガビット データ サービス (SMDS) ネットワークは NBMA と見なすことができることに注意してください。これらのネットワークは、インターフェイスで物理マルチキャストを使用するように設定されていない場合 NBMA と見なされ、それ以外の場合、NBMA とは見なされません。

Examples

次に、イーサネット インターフェイスの 0 の hello インターバルを 10 秒に設定する例を示します。

```
Device (config)#interface ethernet 0
Device (config-if)#ip hello-interval eigrp 109 10
```

Related Commands	Command	Description
	bandwidth (interface)	インターフェイスの帯域幅値を設定します。
	ip hold-time eigrp	自律システム番号によって指定された特定の EIGRP ルーティングプロセスのホールドタイムを設定します。

ip hold-time eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) プロセスのホールドタイムを設定するには、インターフェイス コンフィギュレーション モードで **ip hold-time eigrp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ip hold-time eigrp *as-number seconds*
no ip hold-time eigrp *as-number seconds*

Syntax Description	
<i>as-number</i>	自律システム (AS) 番号。
<i>seconds</i>	ホールド時間 (秒単位)。有効な範囲は 1 ~ 65535 です。

Command Default EIGRP ホールドタイムは、低速の非ブロードキャストマルチアクセス (NBMA) ネットワークで 180 秒で、その他のすべてのネットワークでは 15 秒です。

Command Modes インターフェイス コンフィギュレーション (config-if) 仮想ネットワーク インターフェイス (config-if-vnet)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 非常に混雑した大規模ネットワークでは、一部のルータおよびアクセス サーバが、デフォルト ホールドタイム内にネイバーから hello パケットを受信できない可能性があります。この場合、ホールドタイムを増やすこともできます。

ホールドタイムは、少なくとも hello 間隔の 3 倍にすることを推奨します。指定されたホールド時間内にルータが hello パケットを受信しなかった場合は、そのルータ経由のルートが使用できないと判断されます。

ホールドタイムを増やすと、ネットワーク全体のルート収束が遅くなります。

デフォルトの 180 秒のホールドタイムと 60 秒の hello インターバルは、低速の NBMA メディアだけに適用されます。低速とは、**bandwidth** インターフェイス コンフィギュレーション コマンドで指定されているように、T1 以下のレートのことを指します。

Examples

次に、イーサネット インターフェイス 0 のホールドタイムを 40 秒に設定する例を示します。

```
Device(config)#interface ethernet 0
Device(config-if)#ip hold-time eigrp 109 40
```

Related Commands

Command	Description
bandwidth (interface)	インターフェイスの帯域幅値を設定します。
ip hello-interval eigrp	自律システム番号によって指定された EIGRP ルーティング プロセスの hello インターバルを設定します。

ip load-sharing

インターフェイスで Cisco Express Forwarding のロードバランシングを有効にするには、インターフェイス コンフィギュレーションモードで **ip load-sharing** コマンドを使用します。インターフェイスで Cisco Express Forwarding のロードバランシングを無効にするには、このコマンドの **no** 形式を使用します。

```
ip load-sharing { per-destination }
no ip load-sharing
```

Syntax Description

per-destination	インターフェイスで Cisco Express Forwarding の宛先別ロードバランシングを有効にします。
------------------------	--

Command Default

宛先単位のロードバランシングは、シスコ エクスプレス フォワーディングをイネーブルにすると、デフォルトでイネーブルになります。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

宛先別ロードバランシングにより、デバイスは複数の等コストのパスを使用して負荷を分散させます。指定された送信元と宛先ホストのペアは、複数の等コストのパスを使用可能な場合であっても、同じパスを使用することが保証されています。異なる送信元と宛先ホストのペア宛てのトラフィックは、それぞれ異なるパスを通る傾向があります。

Examples

次の例は、宛先単位のロードバランシングをイネーブルにする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip load-sharing per-destination
```

ip network-broadcast

network-prefix-directedブロードキャストパケットを受信して受け入れるには、デバイスのインターフェイスで **ip network-broadcast** コマンドを設定します。

```
ip network-broadcast
```

Syntax Description このコマンドには、引数またはキーワードはありません。

Command Default このコマンドは、デフォルトでディセーブルになっています。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

Usage Guidelines 出力インターフェイスで **ip directed-broadcast** コマンドを設定する前に、入力インターフェイスで **ip network-broadcast** コマンドを設定します。これにより、ネットワークプレフィックス宛てのブロードキャストパケットが確実に受信され、受け入れられます。

ip network-broadcast コマンドはデフォルトでは無効になっています。このコマンドを設定しない場合、network-prefix-directedブロードキャストパケットはサイレントに廃棄されます。

例

次に、ネットワークが入力で network-prefix-directedブロードキャストパケットを受け入れ、出力インターフェイスでダイレクトブロードキャストから物理ブロードキャストへの変換を設定する方法の例を示しています。

```
Device# configure terminal
Device(config)#interface gigabitethernet 1/0/2
Device(config-if)#ip network-broadcast
Device(config-if)#exit
Device(config)#interface gigabitethernet 1/0/3
Device(config-if)#ip directed-broadcast
Device(config-if)#exit
```

ip ospf database-filter all out

Open Shortest Path First (OSPF) インターフェイスへの発信リンクステートアドバタイズメント (LSA) をフィルタ処理するには、インターフェイスまたは仮想ネットワーク インターフェイス コンフィギュレーション モードで **ip ospf database-filter all out** コマンドを使用します。インターフェイスに対する LSA の転送を元に戻すには、このコマンドの **no** 形式を使用します。

ip ospf database-filter all out [disable]
no ip ospf database-filter all out

Syntax Description

disable	(任意) OSPF インターフェイスへの発信 LSA のフィルタリングを無効にします。すべての発信 LSA がインターフェイスにフラッドイングされます。 Note このキーワードは、仮想ネットワーク インターフェイス モードでのみ使用できます。
----------------	--

Command Default

このコマンドは、デフォルトでディセーブルになっています。すべての発信 LSA がインターフェイスにフラッドイングされます。

Command Modes

インターフェイス コンフィギュレーション (config-if)
 仮想ネットワーク インターフェイス (config-if-vnet)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、**neighbor database-filter** コマンドがネイバーベースで実行する機能と同じ機能を実行します。

仮想ネットワークに対して **ip ospf database-filter all out** コマンドを有効にして無効にする場合は、仮想ネットワーク インターフェイス コンフィギュレーション モードで **disable** キーワードを使用します。

Examples

次に、イーサネット インターフェイス 0 経由で到達可能なブロードキャスト、非ブロードキャスト、ポイントツーポイント ネットワークに OSPF LSA がフィルタリングされないようにする例を示します。

```
Device(config)#interface ethernet 0
Device(config-if)#ip ospf database-filter all out
```

Related Commands

Command	Description
neighbor database-filter	OSPF ネイバーへの発信 LSA をフィルタします。

ip ospf name-lookup

すべての OSPF **show EXEC** コマンド表示で使用するドメインネームシステム（DNS）名を検索するように Open Shortest Path First（OSPF）を設定するには、グローバル コンフィギュレーション モードで **ip ospf name-lookup** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ip ospf name-lookup
no ip ospf name-lookup

Syntax Description このコマンドには、引数またはキーワードはありません。

Command Default このコマンドは、デフォルトでディセーブルになっています。

Command Modes グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドを使用するとルータがルータ ID やネイバー ID ではなく名前が表示されるため、ルータを識別しやすくなります。

Examples 次に、すべての OSPF **show EXEC** コマンドの表示で使用する DNS 名を検索するように OSPF を設定する例を示します。

```
Device(config)#ip ospf name-lookup
```

ip split-horizon eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) スプリットホライズンをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip split-horizon eigrp** コマンドを使用します。スプリットホライズンをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip split-horizon eigrp *as-number*
no ip split-horizon eigrp *as-number*

Syntax Description

<i>as-number</i>	自律システム (AS) 番号。
------------------	-----------------

Command Default

このコマンドの動作は、デフォルトでイネーブルです。

Command Modes

インターフェイス コンフィギュレーション (config-if)
 仮想ネットワーク インターフェイス (config-if-vnet)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

設定で EIGRP スプリット ホライズンをディセーブルにするには、**no ip split-horizon eigrp** コマンドを使用します。

Examples

次の例に、EIGRP スプリット ホライズンを有効にする方法を示します。

```
Device(config-if)#ip split-horizon eigrp 101
```

Related Commands

Command	Description
ip split-horizon (RIP)	スプリット ホライズン メカニズムをイネーブルにします。
neighbor (EIGRP)	ルーティング情報を交換するネイバールータを定義します。

ip summary-address eigrp

指定されたインターフェイスで Enhanced Interior Gateway Routing Protocol (EIGRP) のアドレス集約を設定するには、インターフェイスコンフィギュレーションまたは仮想ネットワークインターフェイスコンフィギュレーションモードで **ip summary-address eigrp** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

ip summary-address eigrp *as-number ip-address mask [admin-distance] [leak-map name]*
no ip summary-address eigrp *as-number ip-address mask*

Syntax Description

<i>as-number</i>	自律システム (AS) 番号。
<i>ip-address</i>	インターフェイスに適用されるサマリー IP アドレス。
<i>mask</i>	サブネット マスク。
<i>admin-distance</i>	(任意) アドミニストレーティブ ディスタンス。範囲は 0 ~ 255 です。 Note Cisco IOS XE リリース 3.2S 以降、 <i>admin-distance</i> 引数が削除されました。アドミニストレーティブ ディスタンスを設定するには、 summary-metric コマンドを使用します。
leak-map <i>name</i>	(任意) サマリー経由でリークするルートを設定するために使用されるルートマップ参照を指定します。

Command Default

- EIGRP サマリー ルートには、アドミニストレーティブ ディスタンス 5 が適用されます。
- EIGRP は、単一ホスト ルートに対しても、自動的にネットワーク レベルを集約します。
- 事前設定されるサマリー アドレスはありません。
- EIGRP のデフォルトのアドミニストレーティブ ディスタンス メトリックは 90 です。

Command Modes

インターフェイス コンフィギュレーション (config-if)

仮想ネットワーク インターフェイス コンフィギュレーション (config-if-vnet)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

インターフェイスレベルのアドレス集約を設定するには、**ip summary-address eigrp** コマンドを使用します。EIGRP 集約ルートには、アドミニストレーティブ ディスタンス値 5 が割り当てられます。アドミニストレーティブ ディスタンス メトリックは、ルーティング テーブルにインストールすることなくサマリーをアドバタイズするために使用します。

デフォルトでは、EIGRPはサブネットルートをネットワークレベルに集約します。**no auto-summary** コマンドを入力して、サブネットレベルの集約を設定することができます。

アドミニストレーティブディスタンスが255に設定されている場合、サマリーアドレスはピアにアドバタイズされません。

リークするルートに対する EIGRP のサポート

キーワード**leak-map**を設定すると、マニュアルサマリーによって抑制されるコンポーネントルートをアドバタイズできるようになります。サマリーの任意のコンポーネントサブセットをリークできます。ルートマップおよびアクセスリストは、リークされたルートを特定するために定義する必要があります。

不完全な設定を入力した場合、次がデフォルトの動作になります。

- 存在しないルートマップを参照するようにキーワード**leak-map**を設定する場合、このキーワードの設定は無効です。サマリーアドレスはアドバタイズされますが、すべてのコンポーネントルートは抑制されます。
- キーワード**leak-map**を設定していてもアクセスリストが存在しないかルートマップがアクセスリストを参照していない場合、サマリーアドレスおよびすべてのコンポーネントルートがアドバタイズされます。

仮想ネットワーク トランク インターフェイスを設定していて **ip summary-address eigrp** コマンドを設定している場合、アドミニストレーティブディスタンス オプションは仮想ネットワーク サブインターフェイス上の **ip summary-address eigrp** コマンドでサポートされていないため、コマンドの *admin-distance* 値はトランクインターフェイス上で実行されている仮想ネットワークによって継承されません。

Examples

次の例は、イーサネット インターフェイス 0/0 で 192.168.0.0/16 サマリーアドレスにアドミニストレーティブディスタンスを95に設定する方法を示しています。

```
Device(config)#router eigrp 1
Device(config-router)#no auto-summary
Device(config-router)#exit
Device(config)#interface Ethernet 0/0
Device(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.0.0 95
```

次に、10.2.2.0 サマリーアドレスを通じてリークされる 10.1.1.0/24 サブネットを設定する例を示します。

```
Device(config)#router eigrp 1
Device(config-router)#exit
Device(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Device(config)#route-map LEAK-10-1-1 permit 10
Device(config-route-map)#match ip address 1
Device(config-route-map)#exit
Device(config)#interface Serial 0/0
Device(config-if)#ip summary-address eigrp 1 10.2.2.0 255.0.0.0 leak-map LEAK-10-1-1
Device(config-if)#end
```

次の例では、GigabitEthernet インターフェイス 0/0/0 を仮想ネットワーク トランク インターフェイスとして設定します。

```
Device(config)#interface gigabitethernet 0/0/0
Device(config-if)#vnet global
Device(config-if-vnet)#ip summary-address eigrp 1 10.3.3.0 255.0.0.0 33
```

Related Commands

Command	Description
auto-summary (EIGRP)	ネットワークレベルのルートにサブネットルートの自動集約を設定します（デフォルト動作）。
summary-metric	EIGRP サマリー集約アドレスの固定メトリックを設定します。

ip route static bfd

スタティックルートの Bidirectional Forwarding Detection (BFD) ネイバーを指定するには、グローバル コンフィギュレーション モードで **ip route static bfd** コマンドを使用します。スタティックルートの BFD ネイバーを削除するには、このコマンドの **no** 形式を使用します。

```
ip route static bfd { interface-type interface-number ip-address | vrf vrf-name } [group group-name]
[passive] [unassociate]
no ip route static bfd { interface-type interface-number ip-address | vrf vrf-name } [group group-name]
[passive] [unassociate]
```

Syntax Description		
<i>interface-type interface-number</i>		インターフェイスのタイプと番号。
<i>ip-address</i>		A.B.C.D 形式のゲートウェイの IP アドレス。
vrf vrf-name		Virtual Routing and Forwarding (VRF) インスタンスと宛先の vrf 名を指定します。
group group-name		(任意) BFD グループを割り当てます。group-name は BFD グループ名を指定する最大 32 文字の文字列です。
unassociate		(任意) BFD に設定されたスタティックルートの関連付けを解除します。

Command Default スタティック ルート BFD ネイバーは指定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines スタティック ルート BFD ネイバーを指定するには、ip route static bfd コマンドを使用します。設定に指定されている同一のインターフェイスとゲートウェイを保持するスタティック ルートはすべて、到達可能性通知を得るために同一の BFD セッションを共有します。

interface-type interface-number および *ip-address* 引数に同じ値が指定されているスタティック ルートはすべて、自動的に BFD を使用して、ゲートウェイの到達可能性を判別し、高速障害検出を利用します。

group キーワードは BFD グループを割り当てます。スタティック BFD 設定は、インターフェイスが関連付けられている VPN ルーティングおよび転送 (VRF) インスタンスに追加されます。**passive** キーワードは、グループのパッシブメンバを指定します。**passive** キーワードなしでグループにスタティック BFD を追加すると、BFD がグループのアクティブメンバになります。グループの BFD セッションをトリガーするために、スタティックルートをアクティブ BFD 設定によって追跡する必要があります。特定のグループのすべてのスタティック BFD 設定 (アクティブとパッシブ) を削除するには、**no ip route static bfd** コマンドを使用して、BFD グループ名を指定します。

unassociate キーワードは、BFD ネイバーがスタティックルートに関連付けられることなく、インターフェイスに BFD が設定されている場合に BFD セッションが要求されることを指定します。これは IPv4 スタティックルートがない BFDv4 セッションを起動するために役立ちます。**unassociate** キーワードを指定しない場合は、IPv4 スタティックルートが BFD セッションに関連付けられます。

BFD では、両方のエンドポイント デバイス BFD セッションが開始されている必要があります。そのため、このコマンドは各エンドポイント デバイスで設定する必要があります。

スイッチ仮想インターフェイス (SVI) の BFD スタティック セッションは、その SVI 上で無効だった **bfd interval milliseconds min_rx milliseconds multiplier multiplier-value** コマンドが有効化された後のみ確立されます。

スタティック BFD セッションを有効にするには、次の手順を実行します。

1. SVI で BFD タイマーを有効にします。

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

2. スタティック IP ルートの BFD を有効にします。

```
ip route static bfd interface-type interface-number ip-address
```

3. SVI で BFD タイマーを無効にし、再度有効にします。

```
no bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

Examples

次に、指定したネイバー、グループおよびグループのアクティブメンバを介してすべてのスタティック ルートの BFD を設定する例を示します。

```
Device#configuration terminal
Device(config)#ip route static bfd GigabitEthernet 1/0/1 10.1.1.1 group group1
```

次に、指定したネイバー、グループおよびグループのパッシブメンバを介してすべてのスタティック ルートの BFD を設定する例を示します。

```
Device#configuration terminal
Device(config)#ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 group group1 passive
```

次に、**group** および **passive** キーワードを指定せず、無関係なモードですべてのスタティック ルートの BFD を設定する例を示します。

```
Device#configuration terminal
Device(config)#ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 unassociate
```

ipv6 route static bfd

スタティックルートの Bidirectional Forwarding Detection for IPv6 (BFDv6) ネイバーを指定するには、グローバルコンフィギュレーションモードで **ipv6 route static bfd** コマンドを使用します。スタティックルートの BFDv6 ネイバーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 route static bfd [**vrf vrf-name**] *interface-type interface-number ipv6-address* [**unassociated**]
no ipv6 route static bfd

Syntax Description	vrf vrf-name	(任意) スタティックルートを指定する必要がある Virtual Routing and Forwarding (VRF) インスタンスの名前。
	<i>interface-type interface-number</i>	インターフェイスのタイプと番号。
	<i>ipv6-address</i>	ネイバーの IPv6 アドレス。
	unassociated	(任意) スタティック BFD ネイバーを関連付けられたモードから無関係なモードに移行します。

Command Default スタティック ルートの BFDv6 ネイバーは指定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines スタティックルートのネイバーを指定するには、**ipv6 route static bfd** コマンドを使用します。設定に指定されている同一のインターフェイスとゲートウェイを保持するスタティックルートはすべて、到達可能性通知を得るために同一の BFDv6 セッションを共有します。BFDv6 では、両方のエンドポイントのルータで BFDv6 セッションが開始されている必要があります。そのため、このコマンドは各エンドポイントルータで設定する必要があります。IPv6 スタティック BFDv6 ネイバーは、インターフェイスとネイバーアドレスで完全に指定される必要があります、直接接続されている必要があります。

vrf vrf-name、interface-type interface-number および ipv6-address に同じ値が指定されているスタティックルートはすべて、自動的に BFDv6 を使用して、ゲートウェイの到達可能性を判別し、高速障害検出を利用します。

Examples

次に、アドレスが 2001::1 のイーサネット インターフェイス 0/0 でネイバーを作成する例を示します。

```
Device#configuration terminal
Device(config)#ipv6 route static bfd ethernet 0/0 2001::1
```

次に、ネイバーを無関係なモードに変換する例を示します。

```
Device#configuration terminal
Device(config)#ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

metric weights (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) メトリック計算を調整するには、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで **metric weights** コマンドを使用します。デフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

Router Configuration

```
metric weights tos k1 k2 k3 k4 k5
no metric weights
```

アドレス ファミリ コンフィギュレーション

```
metric weights tos [k1 [k2 [k3 [k4 [k5 [k6]]]]]]
no metric weights
```

Syntax Description

<i>tos</i>	サービスのタイプ。この値は常にゼロである必要があります。
<i>k1 k2 k3 k4 k5 k6</i>	<p>(任意) EIGRP メトリック ベクトルをスカラー量に変換する定数。有効な値は 0 ~ 255 です。デフォルト値は次のとおりです。</p> <ul style="list-style-type: none"> • <i>k1</i>: 1 • <i>k2</i>: 0 • <i>k3</i>: 1 • <i>k4</i>: 0 • <i>k5</i>: 0 • <i>k6</i>: 0 <p>Note アドレスファミリコンフィギュレーションモードでは、値を指定しないと、デフォルト値が設定されます。<i>k6</i> 引数は、アドレスファミリコンフィギュレーションモードでのみサポートされています。</p>

Command Default

EIGRP メトリック K 値がデフォルト値として設定されます。

Command Modes

ルータ コンフィギュレーション (config-router)

アドレス ファミリ コンフィギュレーション (config-router-af)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを使用すると、EIGRP ルーティングおよびメトリックの計算のデフォルト動作を変更して、特定のタイプオブサービス (ToS) の EIGRP メトリック計算の調整が可能になります。

k5 が 0 に等しい場合、次の計算式に従って複合 EIGRP メトリックが計算されます。

$$\text{メトリック} = [k1 * \text{帯域幅} + (k2 * \text{帯域幅}) / (256 - \text{負荷}) + k3 * \text{遅延} + K6 * \text{拡張メトリック}]$$

k5 がゼロに等しくない場合、追加の計算が実行されます。

$$\text{メトリック} = \text{メトリック} * [k5 / (\text{信頼性} + k4)]$$

$$\text{スケールされた帯域幅} = 10^7 / \text{最小インターフェイス帯域幅 (キロビット/秒)} * 256$$

遅延は、クラシックモードでは数十マイクロ秒、名前付きモードではピコ秒単位です。クラシックモードでは、16進数の FFFFFFFF (10進数 4294967295) の遅延は、ネットワークが到達不能であることを示します。名前付きモードでは、16進数 FFFFFFFFFF (10進数 281474976710655) の遅延は、ネットワークが到達不能であることを示します。

信頼性は 255 のフラクションとして指定されます。つまり、255 は 100% の信頼度または完全に安定したリンクであることを示します。

負荷は、255 のフラクションとして指定されます。負荷 255 は、完全に飽和状態のリンクを表します。

Examples

次に、メトリック ウェイトをデフォルトと少し異なる値に設定する例を示します。

```
Device (config) #router eigrp 109
Device (config-router) #network 192.168.0.0
Device (config-router) #metric weights 0 2 0 2 0 0
```

次に、アドレスファミリメトリック ウェイトを ToS: 0、K1: 2、K2: 0、K3: 2、K4: 0、K5: 0、K6: 1 に設定する例を示します。

```
Device (config) #router eigrp virtual-name
Device (config-router) #address-family ipv4 autonomous-system 4533
Device (config-router-af) #metric weights 0 2 0 2 0 0 1
```

Related Commands

Command	Description
address-family (EIGRP)	アドレスファミリ コンフィギュレーションモードを開始して、EIGRP ルーティング インスタンスを設定します。
bandwidth (interface)	インターフェイスの帯域幅値を設定します。
delay (interface)	インターフェイスの遅延値を設定します。
ipv6 router eigrp	IPv6 EIGRP ルーティング プロセスを設定します。
metric holddown	新しい EIGRP ルーティング情報を一定の期間使用されないようにします。

Command	Description
metric maximum-hops	IP ルーティング ソフトウェアによって、コマンド (EIGRP のみ) によって指定されたものよりも多くのホップカウントのあるルートが到達不能ルートとしてアドバタイズされます。
router eigrp	EIGRP ルーティング プロセスを設定します。

neighbor description

説明をネイバーに関連付けるには、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで **neighbor description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

```
neighbor {ip-addresspeer-group-name} description text
no neighbor {ip-addresspeer-group-name} description [text]
```

Syntax Description

<i>ip-address</i>	ネイバーの IP アドレス。
<i>peer-group-name</i>	EIGRP ピアグループ名。この引数は、アドレス ファミリ コンフィギュレーション モードでは利用できません。
<i>text</i>	ネイバーを説明するテキスト（最大 80 文字）。

Command Default

ネイバーの説明はありません。

Command Modes

ルータ コンフィギュレーション (config-router) アドレス ファミリ コンフィギュレーション (config-router-af)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、ネイバーに「peer with example.com」という説明を設定する例を示します。

```
Device(config)#router bgp 109
Device(config-router)#network 172.16.0.0
Device(config-router)#neighbor 172.16.2.3 description peer with example.com
```

次の例では、アドレス ファミリ ネイバーの説明を「address-family-peer」としています。

```
Device(config)#router eigrp virtual-name
Device(config-router)#address-family ipv4 autonomous-system 4453
Device(config-router-af)#network 172.16.0.0
Device(config-router-af)#neighbor 172.16.2.3 description address-family-peer
```

Related Commands

コマンド	説明
address-family (EIGRP)	アドレスファミリ コンフィギュレーションモードを開始して、EIGRP ルーティング インスタンスを設定します。

コマンド	説明
network (EIGRP)	EIGRP ルーティングプロセスのネットワークを指定します。
router eigrp	EIGRP アドレス ファミリ プロセスを設定します。

network (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) ルーティングプロセスのネットワークを指定するには、ルータ コンフィギュレーションモードまたはアドレスファミリ コンフィギュレーションモードで **network** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

```
network ip-address [wildcard-mask]
no network ip-address [wildcard-mask]
```

Syntax Description

<i>ip-address</i>	直接接続されるネットワークの IP アドレス
<i>wildcard-mask</i>	(任意) EIGRP ワイルドカード ビット。ワイルドカード マスクは、サブネット マスクをビット単位で補完するサブネットワークを示します。

Command Default

ネットワークは指定されていません。

Command Modes

ルータ コンフィギュレーション (config-router) アドレス ファミリ コンフィギュレーション (config-router-af)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

EIGRP ルーティングプロセスに対して **network** コマンドが設定されると、ルータは1つ以上のローカルインターフェイスを一致させます。 **network** コマンドは、 **network** コマンドで設定されたアドレスと同じサブネット内にあるアドレスで構成されているローカルインターフェイスのみと一致します。次にルータが一致したインターフェイスを通じてネイバー関係を確立します。ルータに設定可能なネットワーク文 (**network** コマンド) の数に制限はありません。

ネットワークをまとめてグループ化するためのショートカットとしてワイルドカードマスクを使用します。ワイルドカードマスクは、IPアドレスのネットワーク部分のすべてをゼロと一致させます。ワイルドカードマスクは、特定のホスト/IPアドレス、ネットワーク全体、サブネット、さらにはIPアドレスの範囲を対象としています。

アドレスファミリ コンフィギュレーションモードを開始する際、このコマンドは名前付き EIGRP IPv4 設定だけに適用されます。名前付き IPv6 および Service Advertisement Framework (SAF) 設定では、アドレスファミリ コンフィギュレーションモードでこのコマンドをサポートしていません。

Examples

次に、EIGRP 自律システム 1 を設定し、ネットワーク 172.16.0.0 および 192.168.0.0 を通じてネイバーを確立する例を示します。

```
Device (config)#router eigrp 1
Device (config-router)#network 172.16.0.0
```

```
Device(config-router)#network 192.168.0.0  
Device(config-router)#network 192.168.0.0 0.0.255.255
```

次に、EIGRP アドレス ファミリ 自律システム 4453 を設定し、ネットワーク 172.16.0.0 および 192.168.0.0 を通じてネイバーを確立する例を示します。

```
Device(config)#router eigrp virtual-name  
Device(config-router)#address-family ipv4 autonomous-system 4453  
Device(config-router-af)#network 172.16.0.0  
Device(config-router-af)#network 192.168.0.0
```

Related Commands

コマンド	説明
address-family (EIGRP)	アドレスファミリ コンフィギュレーションモードを開始して、EIGRP ルーティング インスタンスを設定します。
router eigrp	EIGRP アドレス ファミリ プロセスを設定します。

nsf (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) の Cisco Nonstop Forwarding (NSF) 動作をイネーブルにするには、ルータ コンフィギュレーション モードまたはアドレスファミリ コンフィギュレーション モードで **nsf** コマンドを使用します。EIGRP NSF をディセーブルにして EIGRP NSF 設定を running-config ファイルから削除するには、このコマンドの **no** 形式を使用します。

nsf
no nsf

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default EIGRP NSF はディセーブルです。

Command Modes ルータ コンフィギュレーション (config-router)
アドレス ファミリ コンフィギュレーション (config-router-af)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **nsf** コマンドは、NSF 対応ルータで EIGRP NSF サポートをイネーブルまたはディセーブルにするために使用します。NSF は、ハイ アベイラビリティをサポートするプラットフォームでのみサポートされています。

Examples 次の例は、NSF をディセーブルにする方法を示しています。

```
Device#configure terminal
Device(config)#router eigrp 101
Device(config-router)#no nsf
Device(config-router)#end
```

次に、EIGRP IPv6 NSF をイネーブルにする例を示します。

```
Device#configure terminal
Device(config)#router eigrp virtual-name-1
Device(config-router)#address-family ipv6 autonomous-system 10
Device(config-router-af)#nsf
Device(config-router-af)#end
```

Related Commands	コマンド	説明
	debug eigrp address-family ipv6 notifications	EIGRP アドレス ファミリの IPv6 イベント通知に関する情報を表示します。

コマンド	説明
debug eigrp nsf	EIGRP ルーティング プロセスの NSF イベントに関する通知と情報を表示します。
debug ip eigrp notifications	EIGRP ルーティング プロセスの情報と通知を表示します。
show ip protocols	アクティブルーティングプロトコルプロセスのパラメータと現在の状態を表示します。
show ipv6 protocols	アクティブ IPv6 ルーティングプロトコルプロセスのパラメータと現在の状態を表示します。
timers graceful-restart purge-time	EIGRP を実行している NSF 認識ルータが、非アクティブなピア用のルートを保持する期間を決定するために、graceful-restart purge-time タイマーを設定します。
timers nsf converge	再起動しているルータが NSF 対応または NSF 認識ピアから end-of-table 通知を待機する最大時間を設定します。
timers nsf signal	初期再起動期間の最大時間を設定します。

offset-list (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) を介して学習されたルートに対する着信および発信メトリックにオフセットを追加するには、ルータコンフィギュレーションモードまたはアドレスファミリトポロジコンフィギュレーションモードで **offset-list** コマンドを使用します。オフセットリストを削除するには、このコマンドの **no** 形式を使用します。

offset-list {*access-list-number**access-list-name*} {**in**|**out**} *offset* [*interface-type interface-number*]
no offset-list {*access-list-number**access-list-name*} {**in**|**out**} *offset* [*interface-type interface-number*]

Syntax Description

<i>access-list-number</i> <i>access-list-name</i>	標準アクセスリスト番号または適用される名前。アクセスリスト番号 0 は、すべてのネットワーク（ネットワーク、プレフィックス、またはルート）を示します。 <i>offset</i> 値が 0 の場合、アクションは実行されません。
in	着信メトリックにアクセスリストが適用されます。
out	発信メトリックにアクセスリストが適用されます。
<i>offset</i>	アクセスリストと一致するネットワークのメトリックに提供されるプラスのオフセット。オフセットが 0 の場合、アクションは実行されません。
<i>interface-type</i>	(任意) オフセットリストが適用されるインターフェイスタイプ。
<i>interface-number</i>	(任意) オフセットリストが適用されるインターフェイス番号。

Command Default

EIGRP を介して学習されたルートに対する着信および発信メトリックに、オフセット値が追加されません。

Command Modes

ルータコンフィギュレーション (config-router) アドレスファミリトポロジコンフィギュレーション (config-router-af-topology)

Command History

Table 119:

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

オフセット値がルーティングメトリックに追加されました。インターフェイスタイプおよびインターフェイス番号のあるオフセットリストは、拡張済みと見なされ、拡張されていないオフセットリストよりも優先されます。したがって、エントリで拡張オフセットリストと通常のオフセットリストが渡される場合、拡張オフセットリストのオフセットがメトリックに追加されます。

Examples

次の例では、ルータによって、アクセス リスト 21 に対してだけ 10 のオフセットがルータの遅延コンポーネントに適用されます。

```
Device(config-router)#offset-list 21 out 10
```

次の例では、ルータによって、イーサネット インターフェイス 0 から学習されたルートに対して 10 のオフセットが適用されます。

```
Device(config-router)#offset-list 21 in 10 ethernet 0
```

次の例では、ルータによって、EIGRP 名前付きコンフィギュレーションのイーサネット インターフェイス 0 から学習されたルートに対して 10 のオフセットが適用されます。

```
Device(config)#router eigrp virtual-name  
Device(config-router)#address-family ipv4 autonomous-system 1  
Device(config-router-af)#topology base  
Device(config-router-af-topology)#offset-list 21 in 10 ethernet0
```

redistribute (IP)

あるルーティングドメインから別のルーティングドメインにルートを再配布するには、該当するコンフィギュレーションモードで **redistribute** コマンドを使用します。(プロトコルに応じて) 再配布のすべてまたは一部を無効にするには、このコマンドの **no** 形式を使用します。プロトコル固有の動作の詳細については、「使用上のガイドライン」の項を参照してください。

```
redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [autonomous-system-number] [metric
{metric-value | transparent}] [metric-type type-value] [match {internal | external 1 | external 2}]
[tag tag-value] [route-map map-tag] [subnets] [nssa-only]
no redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [autonomous-system-number]
[metric {metric-value | transparent}] [metric-type type-value] [match {internal | external 1 |
external 2}] [tag tag-value] [route-map map-tag] [subnets] [nssa-only]
```

Syntax Description

<i>protocol</i>	<p>ルートの再配布元のプロトコルです。次のキーワードのいずれかになります。 application、bgp、connected、eigrp、isis、mobile、ospf、rip、または static[ip]。</p> <p>static [ip] キーワードは、IP スタティックルートを再配布する場合に使用します。 intermediate system-to-intermediate system (IS-IS) プロトコルに再配布する場合は、オプションの ip キーワードを使用します。</p> <p>application キーワードは、あるルーティングドメインから別のルーティングドメインにアプリケーションを再配布するために使用されます。IS-IS、OSPF、ボーダーゲートウェイプロトコル (BGP)、Enhanced Interior Gateway Routing Protocol (EIGRP)、Routing Information Protocol (RIP) など、さまざまなルーティングプロトコルに複数のアプリケーションを再配布できます。</p> <p>connected キーワードは、インターフェイス上で IP アドレスを有効にすることによって自動的に確立されるルートを示します。Open Shortest Path First (OSPF) や IS-IS などのルーティングプロトコルの場合、これらのルータは自律システムに対して外部として再配布されます。</p>
-----------------	---

<i>process-id</i>	<p>(任意) application キーワードの場合、これはアプリケーションの名前です。</p> <p>bgp キーワードまたは eigrp キーワードの場合、これは 16 ビット 10 進数値である自律システム (AS) 番号です。</p> <p>isis キーワードの場合、これはルーティングプロセスのわかりやすい名前を定義する任意のタグ値です。ルーティングプロセスの名前を作成することは、ルーティングを設定するときに名前を使用することを意味します。2 つのルーティングドメインにルータを設定し、この 2 つのドメイン間でルーティング情報を再配布できます。</p> <p>ospf キーワードの場合、ルートの再配布元の該当する OSPF プロセス ID です。この値により、ルーティングプロセスを識別します。この値は 0 以外の 10 進数で指定します。</p> <p>rip キーワードの場合、<i>process-id</i> の値は必要ありません。</p> <p>application キーワードの場合、これはアプリケーションの名前です。</p> <p>デフォルトでは、プロセス ID は定義されません。</p>
level-1	IS-IS 用に、レベル 1 ルートが他の IP ルーティングプロトコルに個別に再配布されることを指定します。
level-1-2	IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティングプロトコルに再配布されることを指定します。
level-2	IS-IS 用に、レベル 2 ルートが他の IP ルーティングプロトコルに個別に再配布されることを指定します。
<i>autonomous-system-number</i>	<p>(オプション) 再配布ルートの自律システム番号です。有効な範囲は 1 ~ 65535 です。</p> <ul style="list-style-type: none"> 4 バイト自律システム (AS) 番号の形式として asdot 表記 (1.0 ~ 65535.65535) のみがサポートされています。 <p>自律システムの番号形式の詳細については、router bgp コマンドを参照してください。</p>

metric <i>metric-value</i>	(オプション) 同じルータ上の一方の OSPF プロセスから他方の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは一方のプロセスから他方のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。デフォルト値は 0 です
metric transparent	(オプション) 再配布ルートのルーティングテーブルメトリックを RIP メトリックとして使用します。
metric-type <i>type value</i>	<p>(オプション) OSPF ルーティング ドメインにアドバタイズされるデフォルトのルートに関連付けられる外部リンク タイプを指定します。次の 2 つの値のいずれかにすることができます。</p> <ul style="list-style-type: none"> • 1: タイプ 1 外部ルート • 2: タイプ 2 外部ルート <p>metric-type を指定しない場合、Cisco IOS ソフトウェアではタイプ 2 外部ルートが採用されます。</p> <p>IS-IS の場合、次の 2 つの値のいずれかになります。</p> <ul style="list-style-type: none"> • internal: 63 以下の IS-IS メトリック。 • external: 64 以上、128 以下の IS-IS メトリック。 <p>デフォルトは internal です。</p>
match { internal external1 external2 }	<p>(任意) OSPF ルートを他のルーティング ドメインに再配布する条件を指定します。次のいずれかを指定できます。</p> <ul style="list-style-type: none"> • internal: 特定の自律システムの内部ルート。 • external 1: 自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • external 2: 自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。 <p>デフォルトは internal です。</p>

tag <i>tag-value</i>	(オプション) 各外部ルートに付加する 32 ビットの 10 進値を指定します。これは OSPF 自体には使用されません。自律システム境界ルータ (ASBR) 間で情報を通信するために使用できます。何も指定しない場合、BGP および外部ゲートウェイプロトコル (EGP) からのルートにはリモート自律システム (AS) 番号が使用され、その他のプロトコルには 0 が使用されます。
route-map	(オプション) この送信元ルーティングプロトコルから現在のルーティングプロトコルへのルートのインポートをフィルタリングするために照会するルートマップを指定します。指定しない場合は、すべてのルートが再配布されます。このキーワードを指定し、ルートマップタグを 1 つも指定しないと、いずれのルートもインポートされません。
<i>map-tag</i>	(オプション) 設定されているルートマップの ID。
subnets	(オプション) OSPF への再配布ルート。 Note キーワードが設定されているかどうかに関係なく、サブネット機能はデフォルトでイネーブルになります。 subnets この自動追加により、クラスレス OSPF ルートが再配布されます。
nssa-only	(オプション) OSPF に再配布されるすべてのルートに対する nssa-only 属性を設定します。

Command Default

ルートの再配布はディセーブルです。

Command Modes

ルータ コンフィギュレーション (config-router)

アドレス ファミリ コンフィギュレーション (config-af)

アドレス ファミリ トポロジ コンフィギュレーション (config-router-af-topology)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

redistribute コマンドの **no** 形式の使用**Caution**

redistribute コマンドに設定したオプションを削除するには、期待する結果が得られるように **redistribute** コマンドの **no** 形式を慎重に使用する必要があります。キーワードを変更または無効にしても、プロトコルによって他のキーワードの状態に影響する場合としない場合があります。

異なるプロトコルでは、**redistribute** コマンドの **no** 形式を異なる方法で導入することを理解することが重要です。

- BGP、OSPF、RIP の設定では、**no redistribute** コマンドは、実行コンフィギュレーションの **redistribute** コマンドから、指定されたキーワードのみを削除します。これらでは、その他のプロトコルから再配布するときに、減算キーワードの方式を使用します。たとえば、BGP で **no redistribute static route-map interior** を設定する場合、ルートマップのみが再配布から除外され、**redistribute static** がフィルタなしでそのまま残ります。
- **no redistribute isis** コマンドは、実行コンフィギュレーションから IS-IS 再配布を削除します。IS-IS は、IS-IS が再配布されているかどうかや、プロトコルを再配布しているかどうかに関係なく、コマンド全体を削除します。
- EIGRP は、EIGRP コンポーネントバージョン rel5 の前は、減算キーワード方式を使用していました。EIGRP コンポーネントバージョン rel5 以降、**no redistribute** コマンドによって、他のプロトコルから再配布するときに **redistribute** コマンド全体が削除されます。
- **router eigrp** コマンドを発行し、**network** サブコマンドを使用してプロセスのネットワークを指定すると、EIGRP ルーティングプロセスが設定されます。EIGRP ルーティングプロセスを設定しておらず、そのような EIGRP プロセスから BGP、OSPF、RIP へのルートの再配布を設定したとします。**no redistribute eigrp** コマンドを使用して **redistribute eigrp** コマンドのパラメータを変更するか無効にする場合、**no redistribute eigrp** コマンドは特定のパラメータの変更または無効化を行うのではなく **redistribute eigrp** コマンド全体を削除します。

redistribute コマンドのその他の使用上のガイドライン

内部メトリックが指定されたリンクステートプロトコルを受信するルータの場合、ルートのコストには、そのルータから再配布するルータまでのコストと宛先に達するまでのアドバタイズされたコストの合計が考慮されます。外部メトリックでは、宛先に達するまでのアドバタイズされたコストだけを考慮します。

IP ルーティングプロトコルから学習したルートは、レベル 1 またはレベル 2 で接続エリアに再配布できます。**level-1-2** キーワードを使用すると、1 つのコマンドでレベル 1 とレベル 2 の両方のルートが許可されます。

再配布されるルーティング情報は、**distribute-list out** ルータ コンフィギュレーション コマンドでフィルタリングする必要があります。これにより、管理者が意図するルートだけが、受信側のルーティングプロトコルに転送されます。

ルータ コンフィギュレーション コマンドの **redistribute** または **default-information** を使用して OSPF ルーティングドメインにルートを再配布した場合、ルータは必ず自動的に ASBR になります。ただし、デフォルトでは、ASBR はデフォルトルートを OSPF ルーティングドメインに生成しません。

OSPF または BGP 以外のプロトコルから OSPF にルートを再配布するときは、**metric-type** キーワードと **type-value** 引数でメトリックが指定されていないと、OSPF ではデフォルトメトリックとして 20 が使用されます。BGP から OSPF にルートを再配布する場合は、デフォルトメトリックとして 1 が使用されます。OSPF プロセスから別の OSPF プロセスにルートを再配布する場合、自律システム (AS) の外部および Not-So-Stubby Area (NSSA) のルートではデフォルトメトリックとして

20 が使用されます。OSPF プロセス間でエリア内およびエリア間のルートを再配布する場合は、再配布元プロセスの内部 OSPF メトリックが再配布先プロセスの外部メトリックとしてアダプタイズされます（この場合にのみ、OSPF へのルートの再配布時にルーティングテーブルのメトリックが維持されます）。



Note `show ip ospf [topology-info]` コマンドは、`subnets` キーワードが設定されているかどうかに関係なく、`subnets` キーワードを表示します。これは、OSPF のサブネット機能がデフォルトでイネーブルになっているためです。

NSSA エリアの内部のルータでは、`nssa-only` キーワードを指定すると、生成されるタイプ 7 NSSA LSA の伝播 (P) ビットがゼロに設定されます。これらの LSA については、エリア境界ルータでタイプ 5 外部 LSA に変換されません。NSSA エリアおよび標準エリアに接続されているエリア境界ルータでは、`nssa-only` キーワードを指定した場合、ルートが NSSA エリアにのみ再配布されます。

`connected` キーワードが設定されたルートでこの `redistribute` コマンドの影響を受けるのは、`network` ルータ コンフィギュレーション コマンドで指定されていないルートです。

`default-metric` コマンドでメトリックを指定しても、接続ルートのアダプタイズに使用するメトリックには影響しません。



Note `redistribute` コマンドで指定された `metric` 値は、`default-metric` コマンドで指定された `metric` 値よりも優先されます。

内部ゲートウェイプロトコル (IGP) または外部ゲートウェイプロトコル (EGP) の BGP へのデフォルトの再配布は、`default-information originate` ルータ コンフィギュレーション コマンドが指定されない限り許可されません。

4 バイト自律システム番号のサポート

シスコが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして `asplain` (たとえば、65538) を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を `asplain` 形式および `asdot` 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを `asdot` 形式に変更するには、`bgp asnotation dot` コマンドを使用します。

Examples

次に、OSPF ルートを BGP ドメインに再配布する例を示します。

```
Device(config)# router bgp 109
Device(config-router)# redistribute ospf
```

次に、EIGRP ルートを OSPF ドメインに再配布する例を示します。

```
Device(config)# router ospf 110
Device(config-router)# redistribute eigrp
```

次に、指定された EIGRP プロセスルートを OSPF ドメインに再配布する例を示します。EIGRP 派生メトリックは 100 に再マッピングされ、RIP ルートは 200 に再マッピングされます。

```
Device(config)# router ospf 109
Device(config-router)# redistribute eigrp 108 metric 100 subnets
Device(config-router)# redistribute rip metric 200 subnets
```

次に、BGP ルートを IS-IS に再配布する例を示します。リンクステートコストが 5 に指定され、メトリックタイプが外部に設定されます。外部というのは、内部メトリックより優先順位が低いことを示します。

```
Device(config)# router isis
Device(config-router)# redistribute bgp 120 metric 5 metric-type external
```

次に、OSPF ドメインにアプリケーションを再配布し、メトリック値 5 を指定する例を示します。

```
Device(config)# router ospf 4
Device(config-router)# redistribute application am metric 5
```

次に、ネットワーク 172.16.0.0 を OSPF 1 の外部 LSA として設定する例を示します。コストは 100 で維持されます。

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 172.16.0.1 255.0.0.0
Device(config-if)# exit
Device(config)# ip ospf cost 100
Device(config)# interface ethernet 1
Device(config-if)# ip address 10.0.0.1 255.0.0.0
!
Device(config)# router ospf 1
Device(config-router)# network 10.0.0.0 0.255.255.255 area 0
Device(config-if)# exit
Device(config-router)# redistribute ospf 2 subnet
Device(config)# router ospf 2
Device(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

次に、BGP ルートを OSPF に再配布し、asplain 形式のローカルの 4 バイト自律システム番号を割り当てる例を示します。

```
Device(config)# router ospf 2
Device(config-router)# redistribute bgp 65538
```

次に、構成で **redistribute connected metric 1000 subnets** コマンドから **connected metric 1000 subnets** オプションを削除して、**redistribute connected** コマンドをそのままにする例を示します。

```
Device(config-router)# no redistribute connected metric 1000 subnets
```

次に、構成で **redistribute connected metric 1000 subnets** コマンドから **metric 1000** オプションを削除して、**redistribute connected subnets** コマンドをそのままにする例を示します。

```
Device(config-router)# no redistribute connected metric 1000
```

次に、構成で **redistribute connected metric 1000 subnets** コマンドから **subnets** オプションを削除して、**redistribute connected metric 1000** コマンドをそのままにする例を示します。

```
Device(config-router)# no redistribute connected subnets
```

次に、**redistribute connected** コマンドと **redistribute connected** コマンドに設定されたすべてのオプションを構成から削除する方法を示します。

```
Device(config-router)# no redistribute connected
```

次に、EIGRP ルートが名前付き EIGRP 構成の EIGRP プロセスに再配布される例を示します。

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute eigrp 6473 metric 1 1 1 1 1
```

次に、EIGRP 構成で再配布を設定および無効化する例を示します。EIGRP の場合、コマンドの **no** 形式は実行コンフィギュレーションから **redistribute** コマンドセット全体を削除することに注意してください。

```
Device(config)# router eigrp 1
Device(config-router)# network 0.0.0.0
Device(config-router)# redistribute eigrp 2 route-map x
Device(config-router)# redistribute ospf 1 route-map x
Device(config-router)# redistribute bgp 1 route-map x
Device(config-router)# redistribute isis level-2 route-map x
Device(config-router)# redistribute rip route-map x

Device(config)# router eigrp 1
Device(config-router)# no redistribute eigrp 2 route-map x
Device(config-router)# no redistribute ospf 1 route-map x
Device(config-router)# no redistribute bgp 1 route-map x
Device(config-router)# no redistribute isis level-2 route-map x
Device(config-router)# no redistribute rip route-map x
Device(config-router)# end
```

```
Device# show running-config | section router eigrp 1
```

```
router eigrp 1
network 0.0.0.0
```

次に、OSPF 構成で再配布を設定または無効化する例を示します。コマンドの **no** 形式は、実行コンフィギュレーションの **redistribute** コマンドから指定されたキーワードのみを削除することに注意してください。

```
Device(config)# router ospf 1
Device(config-router)# network 0.0.0.0
Device(config-router)# redistribute eigrp 2 route-map x
Device(config-router)# redistribute ospf 1 route-map x
Device(config-router)# redistribute bgp 1 route-map x
Device(config-router)# redistribute isis level-2 route-map x
Device(config-router)# redistribute rip route-map x
```

```

Device(config)# router ospf 1
Device(config-router)# no redistribute eigrp 2 route-map x
Device(config-router)# no redistribute ospf 1 route-map x
Device(config-router)# no redistribute bgp 1 route-map x
Device(config-router)# no redistribute isis level-2 route-map x
Device(config-router)# no redistribute rip route-map x
Device(config-router)# end

```

```

Device# show running-config | section router ospf 1

```

```

router ospf 1
 redistribute eigrp 2
 redistribute ospf 1
 redistribute bgp 1
 redistribute rip
 network 0.0.0.0

```

次に、BGP の再配布からルートマップフィルタのみを削除する例を示します。再配布自体はフィルタなしで有効なままになります。

```

Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2 route-map x

```

次に、BGP への EIGRP 再配布を削除する例を示します。

```

Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2

```

Related Commands

Command	Description
default-information originate (OSPF)	OSPF ルーティングドメインにデフォルトルートを生成します。
router bgp	BGP ルーティングプロセスを設定します。
router eigrp	EIGRP アドレス ファミリ プロセスを設定します。

redistribute (IPv6)

あるルーティングドメインから別のルーティングドメインに IPv6 ルートを再配布するには、IPv6 アドレス ファミリ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
redistribute protocol [process-id][include-connected {level-1 | level-1-2 | level-2}][as-number][metric metric-value] {metric-type type-value}[nssa-only][tagtag-value][route-map map-tag]
```

```
no redistribute protocol [process-id][include-connected {level-1 | level-1-2 | level-2}][as-number][metric metric-value] {metric-type type-value}[nssa-only][tagtag-value][route-map map-tag]
```

Syntax Description

<i>protocol</i>	ルートの再配布元のプロトコルです。 bgp 、 connected 、 eigrp 、 isis 、 lisp 、 nd 、 omp 、 ospf (ospfv3)、 rip 、 または static のいずれかのキーワードを指定できます。
<i>process-id</i>	(オプション) bgp キーワードまたは eigrp キーワードの場合、プロセス ID は 16 ビットの 10 進数の自律システム番号です。 isis キーワードの場合、プロセス ID はルーティングプロセスのわかりやすい名前を定義する任意の値です。Intermediate System-to-Intermediate System (IS-IS) プロセスはルータごとに 1 つだけ指定できます。ルーティングプロセスの名前を作成することは、ルーティングを設定するときに名前を使用することを意味します。 ospf キーワードの場合、プロセス ID は IPv6 の Open Shortest Path First (OSPF) ルーティングプロセスをイネーブルにするときに管理目的で割り当てられた番号です。 rip キーワードの場合、プロセス ID は IPv6 Routing Information Protocol (RIP) ルーティングプロセスのわかりやすい名前を定義する任意の値です。
include-connected	(オプション) ソースプロトコルから学習したルートと、ソースプロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲットプロトコルで再配布できるようにします。
level-1	IS-IS 用に、レベル 1 ルートが他の IPv6 ルーティングプロトコルに個別に再配布されることを指定します。
level-1-2	IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IPv6 ルーティングプロトコルに再配布されることを指定します。
level-2	IS-IS 用に、レベル 2 ルートが他の IPv6 ルーティングプロトコルに個別に再配布されることを指定します。
<i>as-number</i>	(オプション) 再配布ルートの自律システム番号です。

metric <i>metric-value</i>	(オプション) 同じルータ上の一方の OSPF プロセスから他方の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは一方のプロセスから他方のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは20です。
metric-type <i>type-value</i>	(オプション) ルーティングドメインにアダタイズされるデフォルトのルートに関連付けられる外部リンクタイプを指定します。次の2つの値のいずれかにすることができます。 <ul style="list-style-type: none"> • 1: タイプ 1 外部ルート • 2: タイプ 2 外部ルート <p>metric-type キーワードに値が指定されていない場合、Cisco IOS ソフトウェアは、タイプ 2 外部ルートを受け入れます。</p>
nssa-only	(オプション) 再配布されるルートを Not-So-Stubby Area (NSSA) に制限します。
tag tag-value	(オプション) 各外部ルートに付加する 32 ビットの 10 進値を指定します。これは OSPF 自体には使用されません。自律システム境界ルータ (ASBR) 間で情報を通信するために使用できます。何も指定しない場合、BGP および外部ゲートウェイプロトコル (EGP) からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。
route-map	(オプション) この送信元ルーティングプロトコルから現在のルーティングプロトコルへのルートのインポートをフィルタリングするためにチェックするルートマップを指定します。route-map キーワードを指定しない場合、すべてのルートが再配布されます。このキーワードを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。
map-tag	(オプション) 設定されているルート マップの ID。

Command Modes

ルータ コンフィギュレーション (config-router) アドレス ファミリ コンフィギュレーション (config-router-af)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが追加された。

Usage Guidelines

キーワードを変更またはディセーブルにしても、他のキーワードの状態には影響しません。

ルートの再配布が **include-connected** キーワードを指定して設定されている場合、それらは IS-IS で無視されます。インターフェイスにおいて IS-IS からプレフィックスがアダタイズされるのは、インターフェイスで IS-IS が実行されている場合かインターフェイスがパッシブとして設定されている場合です。

IPv6 ルーティングプロトコルから学習されたルートは、レベル1ではIPv6 IS-IS、レベル2では接続エリアに再配布されます。**level-1-2** キーワードを使用すると、1つのコマンドでレベル1とレベル2の両方のルートが許可されます。

IPv6 RIP の場合、**redistribute** コマンドを使用すると、スタティックルートが直接接続されたルートのようにアドバタイズされます。



Note スタティックルートを直接接続されたルートとしてアドバタイズする場合、設定に誤りがあるとルーティングループが発生する可能性があります。

再配布された IPv6 RIP ルーティング情報は、ルータ コンフィギュレーションモードの **distribute-list prefix-list** コマンドで常にフィルタリングされます。**distribute-list prefix-list** コマンドを使用することにより、管理者が意図するルートだけが、受信側のルーティングプロトコルに転送されます。



Note IPv6 RIP の **redistribute** コマンドで指定された **metric** 値は、**default-metric** コマンドを使用して指定された **metric** 値よりも優先されます。

IPv4 では、プロトコルを再配布する場合、プロトコルが実行されているインターフェイスのサブネットもデフォルトで再配布されます。IPv6 では、これはデフォルトの動作ではありません。IPv6 でプロトコルが実行されているインターフェイスのサブネットを再配布するには、**include-connected** キーワードを使用します。IPv6 では、送信元プロトコルが BGP の場合、この機能はサポートされません。

no redistribute コマンドを設定すると、クライアントプロトコルが IS-IS または EIGRP の場合にパラメータ設定が無視されます。

IS-IS のレベル1とレベル2を削除すると、IS-IS 再配布が完全に削除されます。IS-IS レベルの設定は **redistribute** コマンドを使用してのみ設定できます。

ルートタイプの値をすべて削除すると、デフォルトの再配布タイプが OSPFv3 に戻ります。

外部ルートが NSSA に再配布されたときに伝搬ビット (P ビット) をクリアするには、**nssa-only** キーワードを指定します。これにより、対応する NSSA 外部リンク ステートアドバタイズメント (LSA) が他のエリアに変換されなくなります。

Examples

次に、IPv6 BGP ルートを再配布するように IPv6 IS-IS を設定する例を示します。メトリックとして 5 を指定し、メトリックタイプを 1 に設定しています。

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute bgp 64500 metric 5 metric-type 1
```

次に、IPv6 BGP ルートを cisco という名前の IPv6 RIP ルーティングプロセスに再配布する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router rip cisco
Device(config-router)# redistribute bgp 42
```

次に、IS-IS for IPv6 ルートを OSPFv3 for IPv6 ルーティングプロセス 1 に再配布する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute isis 1 metric 32 metric-type 1 tag 85
```

redistribute maximum-prefix (OSPF)

Open Shortest Path First (OSPF) に再配布されるプレフィックスの数を制限したり、OSPF に再配布されたプレフィックスが最大数を越えたときに警告メッセージを生成したりするには、ルータ コンフィギュレーション モードで **redistribute maximum-prefix** コマンドを使用します。この値を削除するには、このコマンドの **no** 形式を使用します。

redistribute maximum-prefix *maximum*[*percentage*][*warning-only*]
no redistribute

Syntax Description

<i>maximum</i>	OSPF に再配布できる IP または IPv6 プレフィックスの最大数を指定する 1 ～ 4294967295 の整数。 キーワード warning-only を設定すると、 <i>maximum</i> 値でシステムが警告メッセージのログを記録するまでに OSPF に再配布できるプレフィックスの数が指定されません。再配布数に制限はありません。 OSPF に再配布できる IP または IPv6 プレフィックスの最大数、またはシステムが警告メッセージのログを記録するまでに OSPF に再配布できるプレフィックス数は、キーワード warning-only が指定されているかどうかで異なります。 引数 <i>maximum</i> のデフォルト値はありません。 warning-only キーワードも設定されている場合は、この値によって再配布が制限されることはありません。その場合は、再配布されるプレフィックスがこの値に達すると警告メッセージが記録される、契機となる数に過ぎません。
<i>percentage</i>	(任意) 1 ～ 100 の整数で、警告メッセージが生成されるしきい値として % で指定します。 デフォルトは 75% です。
warning-only	(任意) 引数 <i>maximum</i> で定義されたプレフィックス数を越えたときに警告メッセージのログが記録されるようにします。追加の再配布が防止されることはありません。

Command Default

デフォルトは 75% です。

Command Modes

ルータ コンフィギュレーション (config-router) アドレス ファミリ コンフィギュレーション (config-router-af)

Command History

リリース	変更内
Cisco IOS XE Fuji 16.9.2	このコマンドを 追加した。

Usage Guidelines

ボーダー ゲートウェイ プロトコル (BGP) の OSPF への再配布などにより、大量の IP または IPv6 プレフィックスが OSPF に挿入されると、ネットワークが深刻なフラッディング状態になるおそれがあります。プレフィックスの再配布数を制限すると、この潜在的な問題を回避できます。

redistribute maximum-prefix コマンドを設定した場合は、プレフィックスの再配布数が設定の最大値に達したときに、それ以上のプレフィックスは再配布されません (**warning-only** キーワードが設定されている場合を除きます)。

Examples

次に、プレフィックスの再配布数が 600 の 85% (510 個のプレフィックス) に達した場合とルートの再配布数が 600 に達した場合にそれぞれ警告メッセージを記録するように設定する例を示します。ただし、再配布されるルート数は制限されません。

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 11
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute eigrp 10 subnets
Device(config-router-af)# redistribute maximum-prefix 600 85 warning-only
```

次に、OSPFv3 プロセスに再配布できるプレフィックスの最大数を 10 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 10
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# redistribute maximum-prefix 10
Device(config-router-af)# redistribute connected
```

route-map

ルーティングプロトコル間でルートを再配布する条件を定義するか、ポリシールーティングをイネーブルにするには、グローバルコンフィギュレーションモードで **route-map** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

route-map *map-tag* [**permit** | **deny**] [*sequence-number*] **ordering-seq** *sequence-name*
no route-map *map-tag* [**permit** | **deny**] [*sequence-number*] **ordering-seq** *sequence-name*

Syntax Description	
<i>map-tag</i>	ルートマップ名。
permit	(任意) ルートマップに一致するルートのみを転送または再配布できます。
deny	(任意) ルートマップに一致するルートの転送または再配布をブロックします。
<i>sequence-number</i>	(任意) すでに同じ名前を設定されているルート マップ リスト内の新しいルート マップの位置を指定する番号。
ordering-seq <i>sequence-name</i>	(任意) 指定された文字列に基づいてルートマップを順序付けます。

Command Default ポリシールーティングが有効になっておらず、ルーティングプロトコル間でルートを再配布する条件が設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **route-map** コマンドを使用して、ルート マップ コンフィギュレーション モードを開始します。ルートを再配布するか、またはパケットにポリシールーティングを適用するには、ルートマップを使用します。ここでは、これらの両方の目的について説明します。

再配布

あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布する条件を定義するには、**route-map** グローバルコンフィギュレーションコマンドと、**match** および **set route-map** コンフィギュレーション コマンドを使用します各 **route-map** コマンドには、**match** および **set** コマンドのリストが関連付けられています。**match** コマンドは *match criteria* (現在の **route-map** コマンドで再配布が許可される条件) を指定します。**set** コマンドは、*set actions* (**match** コマンドによって適用される基準が満たされた場合に実行される再配布アクション) を指定します。**route-map** コマンドが有効で、ユーザがアクションを指定しなかった場合、**permit** アクションがデフォルトで適用されます。**no route-map** コマンドは、ルートマップを削除します。

match ルートマップコンフィギュレーションコマンドには、複数の形式があります。**match** コマンドはどのような順序でも実行できます。また、**set** コマンドで指定された *set actions* に従って、ルートが採譜されるようにすべての **match** コマンドが一致している必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルーティングプロセス間でルートを再配布する方法を詳細に制御する必要がある場合にルートマップを使用します。宛先ルーティングプロトコルは **router** グローバルコンフィギュレーションコマンドを使用して指定します。ソースルーティングプロトコルは **redistribute** ルータコンフィギュレーションコマンドを使用して指定します。ルートマップの設定方法の例については、例のセクションを参照してください。

ルートマップに従ってルートを通過する場合は、ルートマップに複数の要素を持たせることができます。**route-map** コマンドに関連した1つ以上の **match** 句に一致しないルートはすべて無視されます。つまり、アウトバウンドルートマップではルートはアドバタイズされず、インバウンドルートマップでは受け入れられません。一部のデータのみを変更する場合は、2つ目のルートマップセクションに明示的に **match** を指定して設定します。

redistribute ルータコンフィギュレーションコマンドでは、*map-tag* 引数で指定されたルートマップを参照します。複数のルートマップで同じマップタグ名を共有できます。

このルートマップの一致基準が満たされた場合、**permit** キーワードが指定されていると、設定アクションに従ってルートが再配布されます。ポリシールーティングの場合、パケットはポリシーに従ってルーティングされます。一致基準が満たされなかった場合、**permit** キーワードが指定されていると、同じマップタグを持つ次のルートマップがテストされます。あるルートが、同じ名前を共有するルートマップセットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。

ルートマップの一致基準が満たされている場合でも、**deny** キーワードが指定されているとルートは再配布されません。ポリシールーティングの場合、パケットはポリシーに従ってルーティングされません。また、同じマップタグ名を共有しているルートマップは検証されません。パケットがポリシールーティングの対象にならない場合、通常の転送アルゴリズムが使用されます。

ポリシー ルーティング

ルートマップには、ポリシールーティングをイネーブルにするというもう1つの用途があります。ポリシールーティングパケットの条件を定義するには、**route-map** コマンドに加えて、**ip policy route-map** または **ipv6 policy route-map** コマンド、**match** および **set** コマンドを使用します。**match** コマンドは、ポリシールーティングが行われる条件を指定します。**set** コマンドは、**match** コマンドによって適用される条件が満たされている場合に実行するルーティングアクションを指定します。明らかな最短パスとは異なる方法でルートパケットにポリシーを適用することを推奨します。

sequence-number 引数を使用した場合の動作は次のとおりです。

- 提供されたタグでエントリが定義されていない場合、*sequence-number* 引数を 10 にしたエントリが作成されます。
- 指定されているタグで定義されているエントリが1つのみの場合、そのエントリが **route-map** コマンドのデフォルトエントリになります。このエントリの *sequence-number* 引数は変わりません。

- 指定されたタグによって複数のエントリが定義されている場合、*sequence-number* 引数が必要であることを伝えるエラーメッセージが表示されます。

no route-map map-tag コマンドが指定されると (*sequence-number* 引数なし)、ルートマップ全体が削除されます。

Examples

次に、ホップカウントが1の Routing Information Protocol (RIP) ルートを Open Shortest Path First (OSPF) に再配布する例を示します。これらのルートは、メトリックが5、メトリックタイプが **type1**、タグが1の外部リンクステートアドバタイズメント (LSA) として OSPF に再配布されます。

```
Device> enable
Device# configure terminal
Device(config)# router ospf 109
Device(config-router)# redistribute rip route-map rip-to-ospf
Device(config-router)# exit
Device(config)# route-map rip-to-ospf permit
Device(config-route-map)# match metric 1
Device(config-route-map)# set metric 5
Device(config-route-map)# set metric-type type1
Device(config-route-map)# set tag 1
```

次に、IPv6 の場合にホップカウントが1の RIP ルートを OSPF に再配布する例を示します。これらのルートは、タグが42、メトリックタイプが **type1** の外部 LSA として OSPF に再配布されます。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 router ospf 1
Device(config-router)# redistribute rip one route-map rip-to-ospfv3
Device(config-router)# exit
Device(config)# route-map rip-to-ospfv3
Device(config-route-map)# match tag 42
Device(config-route-map)# set metric-type type1
```

次の、名前付きコンフィギュレーションの例では、ホップカウントが1の Enhanced Interior Gateway Routing Protocol (EIGRP) アドレスを再配布する方法を示します。これらのアドレスは、メトリックが5、タグが1の外部アドレスとして EIGRP に再配布されます。

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute eigrp 6473 route-map
virtual-name1-to-virtual-name2
Device(config-router-af-topology)# exit-address-topology
Device(config-router-af)# exit-address-family
Device(config-router)# router eigrp virtual-name2
Device(config-router)# address-family ipv4 autonomous-system 6473
Device(config-router-af)# topology base
Device(config-router-af-topology)# exit-af-topology
Device(config-router-af)# exit-address-family
Device(config)# route-map virtual-name1-to-virtual-name2
Device(config-route-map)# match tag 42
Device(config-route-map)# set metric 5
Device(config-route-map)# set tag 1
```

Related Commands

Command	Description
ip policy route-map	インターフェイスでポリシールーティングに使用するルートマップを特定します。
ipv6 policy route-map	インターフェイス上に IPv6 PBR を設定します。
match	ルーティングテーブルからの値と照合します。
router eigrp	EIGRP アドレス ファミリ プロセスを設定します。
set	接続先のルーティングプロトコルの値を設定します。
show route-map	設定されたすべてのルートマップ、または指定した1つのルートマップだけを表示します。

router-id

固定ルータ ID を使用するには、ルータ コンフィギュレーション モードで **router-id** コマンドを使用します。Open Shortest Path First (OSPF) で以前の OSPF ルータ ID の動作を強制するには、このコマンドの **no** 形式を使用します。

router-id *ip-address*
no router-id *ip-address*

Syntax Description

<i>ip-address</i>	IP アドレス形式でのルータ ID。
-------------------	--------------------

Command Default

OSPF ルーティング プロセスは定義されません。

Command Modes

ルータ コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IP アドレス形式で各ルータに任意の値を定義できます。ただし、それぞれ固有のルータ ID にする必要があります。

すでにアクティブになっている（ネイバーが存在する）OSPF ルータ プロセスでこのコマンドを使用すると、次回のリロード時または手動の OSPF プロセスの再起動時に、新しいルータ ID が使用されます。OSPF プロセスを手動で再起動するには、**clear ip ospf** コマンドを使用します。

Examples

次に、固定ルータ ID を指定する例を示します。

```
router-id 10.1.1.1
```

Related Commands

Command	Description
clear ip ospf	OSPF ルーティング プロセス ID に基づいて再配布をクリアします。
router ospf	OSPF ルーティング プロセスを設定します。

router eigrp

EIGRP ルーティングプロセスを設定するには、グローバル コンフィギュレーション モードで **router eigrp** コマンドを使用します。EIGRP ルーティングプロセスを削除するには、このコマンドの **no** 形式を使用します。

```
router eigrp {autonomous-system-numbervirtual-instance-name}
no router eigrp {autonomous-system-numbervirtual-instance-name}
```

Syntax Description

<i>autonomous-system-number</i>	別の EIGRP アドレス ファミリ ルートに対するサービスを識別するための自律システム番号。ルーティング情報にタグを付加するためにも使用されます。有効範囲は 1 ~ 65535 です。
<i>virtual-instance-name</i>	EIGRP 仮想インスタンス名。この名前は、単一ルータ上のすべてのアドレスファミリルータプロセスで一意でなければいけませんが、ルータ間で一意である必要はありません。

Command Default

EIGRP プロセスは設定されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

autonomous-system-number 引数を使用して **router eigrp** コマンドを設定すると、自律システム (AS) 設定と呼ばれる EIGRP 設定が作成されます。EIGRP AS 設定により、ルーティング情報のタギングに使用できる EIGRP ルーティング インスタンスが作成されます。

引数 *virtual-instance-name* を指定して **router eigrp** コマンドを設定すると、EIGRP 名前付きコンフィギュレーションと呼ばれる EIGRP 設定が作成されます。EIGRP 名前付きコンフィギュレーション自体は、EIGRP ルーティング インスタンスを作成しません。EIGRP 名前付きコンフィギュレーションは、ルーティングに使用される、アドレスファミリ コンフィギュレーションを定義する際に必要なベース コンフィギュレーションです。

Examples

次に、EIGRP プロセス 109 を設定する例を示します。

```
Device(config)# router eigrp 109
```

次に、EIGRP アドレスファミリ ルーティング プロセスを設定し、これに *virtual-name* という名前を割り当てる例を示します。

```
Device(config)# router eigrp virtual-name
```

router ospfv3

Open Shortest Path First バージョン 3 (OSPFv3) のルータ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **router ospfv3** コマンドを使用します。

router ospfv3 [*process-id*]

Syntax Description	<i>process-id</i> (任意) 内部ID。ここで使用される番号は、OSPFv3 ルーティングプロセスをイネーブルにするときに管理目的で割り当てられた番号です。範囲は 1 ~ 65535 です。				
Command Default	OSPFv3 ルーティングプロセスはデフォルトではディセーブルになっています。				
Command Modes	グローバル コンフィギュレーション (config)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されま</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されま
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されま				

Usage Guidelines **router ospfv3** コマンドは、OSPFv3 ルータ コンフィギュレーション モードを開始するために使用します。このモードから、IPv6 または IPv4 のアドレスファミリ コンフィギュレーション モードを開始し、IPv6 または IPv4 アドレスファミリを設定できます。

Examples

次に、OSPFv3 ルータ コンフィギュレーション モードを開始する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)#
```

Related Commands	コマンド	説明
	address-family ipv6	IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。

send-lifetime

キーチェーンの認証キーが送信できる期間を設定するには、**send-lifetime** コマンドをキーチェーンキーコンフィギュレーションモードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
send-lifetime [ local ] start-time { infinite end-time | duration seconds }
no send-lifetime
```

Syntax Description

local	ローカルタイムゾーンで時刻を指定します。
<i>start-time</i>	<p>key コマンドで指定したキーが送信できる開始時刻です。構文は次のいずれかにすることができます。</p> <p><i>hh</i> : <i>mm</i> : <i>ss</i> <i>month</i> <i>date</i> <i>year</i></p> <p><i>hh</i> : <i>mm</i> : <i>ss</i> <i>date</i> <i>month</i> <i>year</i></p> <ul style="list-style-type: none"> • <i>hh</i>: 時間 • <i>mm</i>: 分 • <i>ss</i>: 秒 • <i>month</i>: 月の最初の3文字 • <i>date</i>: 日 (1 ~ 31) • <i>year</i>: 年 (4桁) <p>デフォルトの開始時刻で、指定できる最初の日付は1993年1月1日です。</p>
infinite	キーは <i>start-time</i> 値以降、送信可能です。
<i>end-time</i>	キーは、 <i>start-time</i> 値から <i>end-time</i> 値まで、送信可能です。シンタックスは、 <i>start-time</i> 値と同じです。 <i>end-time</i> は <i>start-time</i> 値の後である必要があります。デフォルトの終了時刻は無限の期間です。
duration <i>seconds</i>	キーが送信可能な時間の長さ (秒単位) 指定できる範囲は1 ~ 864000です。

Command Default

期限なし (開始時刻は1993年1月1日、終了時刻は無期限)

Command Modes

キーチェーンキーコンフィギュレーション (config-keychain-key)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

start-time 値と、**infinite**、*end-time*、または **duration** *seconds* のいずれかの値を指定します。

キーにライフタイムを設定する場合は、Network Time Protocol (NTP) または時刻同期方式を実行することを推奨します。

最後のキーが期限切れになった場合、認証は続行されますが、エラーメッセージが生成されず。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

Examples

次の例では、chain1 という名前のキーチェーンが設定されます。Key1 という名前のキーは、午後1時30分から午後3時30分まで承認され、午後2時から午後3時まで送信されます。Key2 という名前のキーは、午後2時30分から午後4時30分まで承認され、午後3時から午後4時まで送信されます。この重複により、キーの移行またはルータの設定時間の不一致に対処できます。時間の違いを処理するために、前後に30分間の余裕が設けられています。

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# ip rip authentication key-chain chain1
Device(config-if)# ip rip authentication mode md5
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# network 172.19.0.0
Device(config-router)# version 2
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain)# key-string key2
Device(config-keychain)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

次に、chain1 という名前のキーをEIGRPアドレスファミリに設定する例を示します。Key1 という名前のキーは、午後1時30分から午後3時30分まで承認され、午後2時から午後3時まで送信されます。Key2 という名前のキーは、午後2時30分から午後4時30分まで承認され、午後3時から午後4時まで送信されます。この重複により、キーの移行またはルータの設定時間の不一致に対処できます。時間の違いを処理するために、前後に30分間の余裕が設けられています。

```
Device(config)# router eigrp 10
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# authentication key-chain trees
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string key2
```

```
Device(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
key	キーチェーンの認証キーを識別します。
key chain	ルーティングプロトコルの認証をイネーブルにするために必要な認証キーチェーンを定義します。
key-string (authentication)	キーの認証文字列を指定します。
show key chain	認証キーの情報を表示します。

show ip eigrp interfaces

Enhanced Interior Gateway Routing Protocol (EIGRP) 用に設定されたインターフェイスに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ip eigrp interfaces** コマンドを使用します。

show ip eigrp [**vrf** *vrf-name*] [*autonomous-system-number*] **interfaces** [*type number*] [**detail**]

Syntax Description	
vrf <i>vrf-name</i>	(任意) 指定された仮想ルーティング/転送 (VRF) インスタンスに関する情報を表示します。
<i>autonomous-system-number</i>	(任意) 出力をフィルタリングする必要がある自律システム番号。
<i>type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>number</i>	(任意) インターフェイスまたはサブインターフェイスの番号です。ネットワークング デバイスに対する番号付け構文の詳細については、疑問符 (?) のオンラインヘルプ機能を使用してください。
detail	(任意) 特定の EIGRP プロセスの EIGRP インターフェイスに関する詳細情報を表示します。

Command Modes ユーザ EXEC (>)

特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines アクティブな EIGRP インターフェイスと EIGRP 固有のインターフェイス設定と統計情報を表示するには、**show ip eigrp interfaces** コマンドを使用します。オプションの *type number* 引数と **detail** キーワードは任意の順序で入力できます。

インターフェイスが指定される場合、そのインターフェイスに関する情報だけが表示されます。それ以外は、EIGRP が動作しているすべてのインターフェイスに関する情報が表示されます。

自律システムが指定された場合、指定された自律システムについてのルーティングプロセスのみが表示されます。指定されない場合、すべての EIGRP プロセスが表示されます。

このコマンドは、EIGRP 名前付きコンフィギュレーションおよび EIGRP 自律システム コンフィギュレーションに関する情報を表示するために使用できます。

このコマンドは、**show eigrp address-family interfaces** コマンドと同じ情報を表示します。シスコでは、**show eigrp address-family interfaces** コマンドを使用することを推奨しています。

Examples

次に、**show ip eigrp interfaces** コマンドの出力例を示します。

```
Device#show ip eigrp interfaces

EIGRP-IPv4 Interfaces for AS(60)

```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Di0	0	0/0	0	11/434	0	0
Et0	1	0/0	337	0/10	0	0
SE0:1.16	1	0/0	10	1/63	103	0
Tu0	1	0/0	330	0/16	0	0

次の **show ip eigrp interfaces detail** コマンドの出力例は、アクティブなすべての EIGRP インターフェイスに関する詳細情報を表示します。

```
Device#show ip eigrp interfaces detail

EIGRP-IPv4 Interfaces for AS(1)

```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Et0/0	1	0/0	0/0	525	0/2	3264	0

Hello-interval is 5, Hold-time is 15
 Split-horizon is enabled
 Next xmit serial <none>
 Packetized sent/expedited: 3/0
 Hello's sent/expedited: 6/2
 Un/reliable mcasts: 0/6 Un/reliable ucasts: 7/4
 Mcast exceptions: 1 CR packets: 1 ACKs suppressed: 0
 Retransmissions sent: 1 Out-of-sequence rcvd: 0
 Topology-ids on interface - 0
 Authentication mode is not set

次の **show ip eigrp interfaces detail** コマンドの出力例は、**no-ecmp-mode** オプションとともに **no ip next-hop self** コマンドが設定されている特定のインターフェイスに関する詳細情報を表示します。

```
Device#show ip eigrp interfaces detail tunnel 0

EIGRP-IPv4 Interfaces for AS(1)

```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu0/0	2	0/0	0/0	2	0/0	50	0

Hello-interval is 5, Hold-time is 15
 Split-horizon is disabled
 Next xmit serial <none>
 Packetized sent/expedited: 24/3
 Hello's sent/expedited: 28083/9
 Un/reliable mcasts: 0/19 Un/reliable ucasts: 18/64
 Mcast exceptions: 5 CR packets: 5 ACKs suppressed: 0
 Retransmissions sent: 52 Out-of-sequence rcvd: 2
 Next-hop-self disabled, next-hop info forwarded, **ECMP mode Enabled**
 Topology-ids on interface - 0
 Authentication mode is not set

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 120: show ip eigrp interfaces フィールドの説明

フィールド	説明
Interface	EIGRP が設定されるインターフェイス。
Peers	直接接続された EIGRP ネイバーの数。
PeerQ Un/Reliable	インターフェイス上の特定のピアに送信するためにキューに入れられた信頼性の低いパケットと信頼性の高いパケットの数。
Xmit Queue Un/Reliable	信頼性の低い送信キューおよび信頼性の高い送信キューに残っているパケットの数。
Mean SRTT	平均スムーズ ラウンドトリップ時間 (SRTT) 間隔 (秒単位)。
Pacing Time Un/Reliable	インターフェイスから EIGRP パケット (信頼性の低いパケットおよび信頼性の高いパケット) を送信するタイミングを決定するために使用されるペーシング時間 (秒単位)。
Multicast Flow Timer	デバイスがマルチキャスト EIGRP パケットを送信する最大秒数。
Pending Routes	送信キュー内で送信を待機しているルートの数。
Packetized sent/expedited	インターフェイス上のネイバーにパケットを送信するために準備された EIGRP ルートの数、および複数のルートが1つのパケットに格納された回数。
Hello's sent/expedited	インターフェイス上で送信された EIGRP hello パケットの数と、迅速化されたパケットの数。

Related Commands

Command	Description
show eigrp address-family interfaces	EIGRP に設定されているアドレス ファミリ インターフェイスに関する情報を表示します。
show ip eigrp neighbors	EIGRP によって検出されたネイバーを表示します。

show ip eigrp neighbors

Enhanced Interior Gateway Routing Protocol (EIGRP) によって検出されたネイバーを表示するには、特権 EXEC モードで **show ip eigrp neighbors** コマンドを使用します。

show ip eigrp [*vrf vrf-name*] [*autonomous-system-number*] **neighbors** [*static|detail*] [*interface-type interface-number*]

Syntax Description		
vrf <i>vrf-name</i>		(任意) 指定された VPN ルーティングおよび転送 (VRF) インスタンスに関する情報を表示します。
<i>autonomous-system-number</i>		(任意) 自律システム番号固有の出力が表示されます。
static		(任意) スタティック ネイバーを表示します。
detail		(任意) 詳細なネイバー情報を表示します。
<i>interface-type interface-number</i>		(任意) インターフェイス固有の出力が表示されます。

Command Modes 特権 EXEC (#)

Command History		変更内容
	リリース	
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ip eigrp neighbors** コマンドは、EIGRP 名前付きコンフィギュレーションおよび EIGRP 自律システム コンフィギュレーションに関する情報を表示するために使用できます。動的および静的ネイバー状態を表示するには、**show ip eigrp neighbors** コマンドを使用します。このコマンドを使用して、特定のタイプのトランスポート問題をデバッグすることもできます。

このコマンドは、**show eigrp address-family neighbors** コマンドと同じ情報を表示します。シスコでは、**show eigrp address-family neighbors** コマンドを使用することを推奨しています。

Examples

次に、**show ip eigrp neighbors** コマンドの出力例を示します。

```
Device#show ip eigrp neighbors

H   Address                Interface           Hold Uptime      SRTT   RTO  Q   Seq
                               (sec)              (ms)              5000    0   5
0   10.1.1.2                 Et0/0              13 00:00:03 1996
2   10.1.1.9                 Et0/0              14 00:02:24 206   5000 0   5
1   10.1.2.3                 Et0/1              11 00:20:39 2202  5000 0   5
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 121: show ip eigrp neighbors フィールドの説明

フィールド	説明
Address	EIGRP ピアの IP アドレス
Interface	ルータがピアから hello パケットを受信するインターフェイス
Hold	ピアのダウンを宣言する前に、EIGRP がピアからのヒアリングを待機する時間（秒）。
Uptime	ローカルルータが最初にこのネイバーからヒアリングしてからの経過時間（時:分:秒）。
SRTT	スムーズラウンドトリップ時間。これは、EIGRP パケットがこのネイバーに送信される際に必要な時間およびローカルルータがそのパケットの確認応答を受信する際にかかる時間（ミリ秒単位）の数字です。
RTO	Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、再送信キューからネイバーへパケットを再送信するまでソフトウェアが待機する時間です。
Q Cnt	ソフトウェアが送信を待機する EIGRP パケット（アップデート、クエリー、応答）の数。
Seq Num	このネイバーから受信した最新アップデート、クエリー、または応答パケットのシーケンス番号。

次に、**show ip eigrp neighbors detail** コマンドの出力例を示します。

```
Device#show ip eigrp neighbors detail
```

```
EIGRP-IPv4 VR(foo) Address-Family Neighbors for AS(1)
H   Address                Interface          Hold Uptime      SRTT   RTO   Q   Seq
   (sec)                   (ms)              Cnt Num
0   192.168.10.1            Gi2/0              12 00:00:21 1600  5000  0   3
  Static neighbor (Lisp Encap)
  Version 8.0/2.0, Retrans: 0, Retries: 0, Prefixes: 1
  Topology-ids from peer - 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 122: show ip eigrp neighbors detail フィールドの説明

フィールド	説明
H	このカラムは、指定されたネイバーとの間で確立されたピアリングセッションの順番を示します。順番は、0 から始まる連続した番号で指定されます。
Address	EIGRP ピアの IP アドレス
Interface	ルータがピアから hello パケットを受信するインターフェイス

フィールド	説明
Hold	ピアのダウンを宣言する前に、EIGRP がピアからのヒアリングを待機する時間（秒）。
Lisp Encap	このネイバーからのルートが LISP によってカプセル化されたことを示します。
Uptime	ローカル ルータが最初にこのネイバーからヒアリングしてからの経過時間（時:分:秒）。
SRTT	スムーズラウンドトリップ時間。これは、EIGRP パケットがこのネイバーに送信される際に必要な時間およびローカルルータがそのパケットの確認応答を受信する際にかかる時間（ミリ秒単位）の数字です。
RTO	Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、再送信キューからネイバーへパケットを再送信するまでソフトウェアが待機する時間です。
Q Cnt	ソフトウェアが送信を待機する EIGRP パケット（アップデート、クエリー、応答）の数。
Seq Num	このネイバーから受信した最新アップデート、クエリー、または応答パケットのシーケンス番号。
Version	指定されたピアが実行中のソフトウェア バージョン。
Retrans	パケットを再送信した回数。
[Retries]	パケットの再送を試行した回数。

Related Commands

Command	Description
show eigrp address-family neighbors	EIGRP によって検出されたネイバーを表示します。

show ip eigrp topology

Enhanced Interior Gateway Routing Protocol (EIGRP) トポロジテーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip eigrp topology** コマンドを使用します。

show ip eigrp topology [*network* [*mask*]*prefix*] **active** | **all-links** | **detail-links** | **frr** | **pending** | **secondary-paths** | **summary** | **zero-successors**]

Syntax Description	
<i>network</i>	(任意) ネットワーク アドレス。
<i>mask</i>	(任意) ネットワーク マスク。
<i>prefix</i>	(任意) <network>/<length> 形式のネットワーク プレフィックス (例: 192.168.0.0/16)。
active	(任意) アクティブ状態にあるすべてのトポロジエントリを表示します。
all-links	(任意) (到達不能な後継ソースを含む) EIGRP トポロジテーブル内の全エントリを表示します。
detail-links	(任意) 追加詳細のあるすべてのトポロジエントリを表示します。
frr	(任意) EIGRP トポロジテーブルに設定されているループフリー代替のリストを表示します。
pending	(任意) ネイバーからのアップデートを待機しているか、ネイバーへの応答を待機している、EIGRP トポロジテーブル内のすべてのエントリを表示します。
secondary-paths	(任意) トポロジのセカンダリパスを表示します。
summary	(任意) EIGRP トポロジテーブルの要約を表示します。
zero-successors	(任意) サクセサがゼロの使用可能なルートを表示します。

Command Default このコマンドがオプションのキーワードなしで使用される場合、フィージブルサクセサのあるトポロジエントリだけが表示され、実行可能なパスだけが表示されます。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History		変更内容
	リリース	
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.1	frr キーワードが導入されました。

Usage Guidelines

show ip eigrp topology コマンドを使用して、トポロジエントリ、実行可能なパス、実行不可能なパス、メトリック、および状態を表示します。このコマンドは、引数またはキーワードなしで使用して、フィージブルサクセサと実行可能なパスを持つトポロジエントリのみを表示することができます。**all-links** キーワードは、実行可能かどうかにかかわらずすべてのパスを表示し、**detail-links** キーワードはこれらのパスに関する追加の詳細を表示します。

EIGRP 名前付きコンフィギュレーションおよび EIGRP 自律システム コンフィギュレーションに関する情報を表示するには、このコマンドを使用します。このコマンドは、**show eigrp address-family topology** コマンドと同じ情報を表示します。シスコでは、**show eigrp address-family topology** コマンドを使用することを推奨しています。

Examples

次に、**show ip eigrp topology** コマンドの出力例を示します。

```
Device# show ip eigrp topology

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status, s - sia status
P 10.0.0.0/8, 1 successors, FD is 409600
   via 192.0.2.1 (409600/128256), Ethernet0/0
P 192.16.1.0/24, 1 successors, FD is 409600
   via 192.0.2.1 (409600/128256), Ethernet0/0
P 10.0.0.0/8, 1 successors, FD is 281600
   via Summary (281600/0), Null0
P 10.0.1.0/24, 1 successors, FD is 281600
   via Connected, Ethernet0/0
```

次の **show ip eigrp topology prefix** コマンドの出力例は、単一のプレフィックスに関する詳細情報を表示します。表示されるプレフィックスは EIGRP 内部ルートです。

```
Device# show ip eigrp topology 10.0.0.0/8

EIGRP-IPv4 VR(vr1) Topology Entry for AS(1)/ID(10.1.1.2) for 10.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 82329600, RIB is 643200
Descriptor Blocks:
10.1.1.1 (Ethernet2/0), from 10.1.1.1, Send flag is 0x0
Composite metric is (82329600/163840), route is Internal
Vector metric:
  Minimum bandwidth is 16000 Kbit
  Total delay is 631250000 picoseconds
  Reliability is 255/255
  Load is 1/55
  Minimum MTU is 1500
  Hop count is 1
  Originating router is 10.1.1.1
```

次の **show ip eigrp topology prefix** コマンドの出力例は、単一のプレフィックスに関する詳細情報を表示します。表示されるプレフィックスは EIGRP 外部ルートです。

```
Device# show ip eigrp topology 192.16.1.0/24

EIGRP-IPv4 Topology Entry for AS(1)/ID(10.0.0.1) for 192.16.1.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600, RIB is 643200
Descriptor Blocks:
192.16.1.0/24 (Ethernet0/0), from 10.0.1.2, Send flag is 0x0
Composite metric is (409600/128256), route is External
Vector metric:
  Minimum bandwidth is 10000 Kbit
```

```

Total delay is 6000 picoseconds
Reliability is 255/255
Load is 1/5
Minimum MTU is 1500
Hop count is 1
Originating router is 192.16.1.0/24
External data:
AS number of route is 0
External protocol is Connected, external metric is 0
Administrator tag is 0 (0x00000000)

```

次の **show ip eigrp topology prefix** コマンドの出力例は、EIGRP トポロジで **no-ecmp-mode** キーワードを指定しないで **no ip next-hop-self** コマンドを設定した場合の等コストマルチパス (ECMP) モード情報を表示します。ECMP モードは、アドバタイズされているパスに関する情報を提供します。複数のサクセサが存在する場合、一番上のパスがすべてのインターフェイス上のデフォルトパスとしてアドバタイズされ、出力に「**ECMP Mode: Advertise by default**」と表示されます。デフォルトパス以外のパスがアドバタイズされる場合は、「**ECMP Mode: Advertise out <Interface name>**」と表示されます。

トポロジテーブルには、特定のプレフィックスのルートエントリが表示されます。ルートは、メトリック、ネクストホップ、およびインフォソースに基づいてソートされます。Dynamic Multipoint VPN (DMVPN) シナリオでは、同じメトリックとネクストホップを持つルートがインフォソースに基づいてソートされます。ECMP のトップルートは常にアドバタイズされます。

```
Device# show ip eigrp topology 192.168.10.0/24
```

```

EIGRP-IPv4 Topology Entry for AS(1)/ID(10.10.100.100) for 192.168.10.0/24
State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
Descriptor Blocks:
  10.100.1.0 (Tunnel0), from 10.100.0.1, Send flag is 0x0
    Composite metric is (284160/281600), route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 1100 microseconds
      Reliability is 255/255
      Load is 1/5
      Minimum MTU is 1400
      Hop count is 1
      Originating router is 10.10.1.1
      ECMP Mode: Advertise by default
  10.100.0.2 (Tunnel1), from 10.100.0.2, Send flag is 0x0
    Composite metric is (284160/281600), route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 1100 microseconds
      Reliability is 255/255
      Load is 1/5
      Minimum MTU is 1400
      Hop count is 1
      Originating router is 10.10.2.2
      ECMP Mode: Advertise out Tunnel1

```

次の **show ip eigrp topology all-links** コマンドの出力例は、実行可能でないものを含むすべてのパスを表示します。

```
Device# show ip eigrp topology all-links
```

```
EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 172.16.1.0/24, 1 successors, FD is 409600, serno 14
   via 10.10.1.2 (409600/128256), Ethernet0/0
   via 10.1.4.3 (2586111744/2585599744), Serial3/0, serno 18
```

次の **show ip eigrp topology detail-links** コマンドの出力例は、ルートに関する追加の詳細情報を表示します。

```
Device# show ip eigrp topology detail-links

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/8, 1 successors, FD is 409600, serno 6
   via 10.10.1.2 (409600/128256), Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 409600, serno 14
   via 10.10.1.2 (409600/128256), Ethernet0/0
P 10.0.0.0/8, 1 successors, FD is 281600, serno 3
   via Summary (281600/0), Null0
P 10.1.1.0/24, 1 successors, FD is 281600, serno 1
   via Connected, Ethernet0/0
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 123: show ip eigrp topology フィールドの説明

フィールド	説明
Codes	<p>このトポロジテーブルエントリの状態。Passive および Active は、宛先に関する EIGRP 状態を参照します。Update、Query、および Reply は、送信されているパケットのタイプを参照します。</p> <ul style="list-style-type: none"> • P - Passive: このルートに対して EIGRP 計算が実行されていないことを示します。 • A - Active: このルートに対して EIGRP 計算が実行されていることを示します。 • U - Update: このルートに対して保留アップデートパケットが送信を待機していることを示します。 • Q - Query: このルートに対して保留クエリーパケットが送信を待機していることを示します。 • R - Reply: このルートに対して保留応答パケットが送信を待機していることを示します。 • r - Reply status: EIGRP がこのルートに対してクエリーを送信し、指定されたパスからの応答を待機しています。 • s - sia status: EIGRP クエリーパケットが stuck-in-active (SIA) ステータスであることを示します。
successors	<p>サクセサの数。この数値は、IP ルーティングテーブル内のネクストホップの数に対応します。successors が大文字で表示される場合、ルートまたはネクストホップは遷移状態です。</p>
serno	シリアル番号。

フィールド	説明
FD	フィジブルディスタンス。フィジブルディスタンスは、宛先に到達するための最適なメトリックか、ルートがアクティブになったときに認識された最適なメトリックです。この値はフィジビリティ条件チェックに使用されます。レポートされたデバイスのディスタンスがフィジブルディスタンス未満の場合、フィジビリティコンディションが満たされて、そのルートはフィジブルサクセサになります。ソフトウェアは、パスをフィジブルサクセサだと判断した後は、その宛先にクエリーを送信する必要はありません。
via	パッシブルートをアダバタイズするネクストホップアドレス。

Related Commands

コマンド	説明
show eigrp address-family topology	EIGRP アドレスファミリ トポロジテーブル内のエントリを表示します。

show ip eigrp traffic

送受信した Enhanced Interior Gateway Routing Protocol (EIGRP) パケット数を表示するには、特権 EXEC モードで **show ip eigrp traffic** コマンドを使用します。

show ip eigrp [vrf {vrf-name |*}] [autonomous-system-number] traffic

Syntax Description

vrf <i>vrf-name</i>	(任意) 指定された VRF に関する情報を表示します。
vrf *	(任意) すべての VRF に関する情報を表示します。
<i>autonomous-system-number</i>	(任意) 自律システム番号。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、EIGRP 名前付きコンフィギュレーションおよび EIGRP 自律システム (AS) コンフィギュレーションに関する情報を表示するために使用できます。

このコマンドは、**show eigrp address-family traffic** コマンドと同じ情報を表示します。シスコでは、**show eigrp address-family traffic** コマンドを使用することを推奨しています。

Examples

次に、**show ip eigrp traffic** コマンドの出力例を示します。

```
Device#show ip eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS(60)
Hellos sent/received: 21429/2809
Updates sent/received: 22/17
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 16/13
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 204
PDM Process ID: 203
Socket Queue: 0/2000/2/0 (current/max/highest/drops)
Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 124: show ip eigrp traffic フィールドの説明

フィールド	説明
Hellos sent/received	送受信された hello パケットの数
Updates sent/received	送受信されたアップデートパケットの数

show ip eigrp traffic

フィールド	説明
Queries sent/received	送受信されたクエリー パケットの数
Replies sent/received	送受信された応答パケットの数
Acks sent/received	送受信される確認応答パケットの数
SIA-Queries sent/received	送受信される Stuck in Active クエリー パケット数
SIA-Replies sent/received	送受信される Stuck in Active 応答パケットのスタック数
Hello Process ID	hello プロセス ID
PDM Process ID	プロトコル依存モジュール IOS プロセス ID
Socket Queue	IP から EIGRP hello プロセスへのソケット キュー カウンタ
Input queue	EIGRP hello プロセスから EIGRP PDM へのソケット キュー カウンタ

Related Commands

Command	Description
show eigrp address-family traffic	送受信された EIGRP パケットの数を表示します。

show ip ospf

Open Shortest Path First (OSPF) ルーティングプロセスに関する一般情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ip ospf** コマンドを使用します。

show ip ospf [*process-id*]

Syntax Description

<i>process-id</i>	(任意) プロセス ID。この引数を指定すると、指定されたルーティングプロセスの情報だけが追加されます。
-------------------	--

Command Modes

ユーザ EXEC、特権 EXEC

Command History

メインライン リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、特定の OSPF プロセス ID を指定しないで入力されたときの、**show ip ospf** コマンドの出力例を示します。

```
Device#show ip ospf

Routing Process "ospf 201" with ID 10.0.0.1 and Domain ID 10.20.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 100 secs
Interface flood pacing timer 55 msec
Retransmission pacing timer 100 msec
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has message digest authentication
    SPF algorithm executed 4 times
    Area ranges are
    Number of LSA 4. Checksum Sum 0x29BEB
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 3
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
  Area 172.16.26.0
    Number of interfaces in this area is 0
    Area has no authentication
    SPF algorithm executed 1 times
    Area ranges are
      192.168.0.0/16 Passive Advertise
    Number of LSA 1. Checksum Sum 0x44FD
```

```

Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 1
Number of indication LSA 1
Number of DoNotAge LSA 0
Flood list length 0

```

Cisco IOS Release 12.2(18)SXE、12.0(31)S、および 12.4(4)T

次に、BFD機能がOSPFプロセス123でイネーブルされているかどうかを確認する **show ip ospf** コマンドの出力例を示します。この出力では、対応するコマンド出力が太字で表示されています。

```
Device#show ip ospf
```

```

Routing Process "ospf 123" with ID 172.16.10.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
BFD is enabled
Area BACKBONE(0)
Number of interfaces in this area is 2
Area has no authentication
SPF algorithm last executed 00:00:03.708 ago
SPF algorithm executed 27 times
Area ranges are
Number of LSA 3. Checksum Sum 0x00AEF1
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 125: show ip ospf フィールドの説明

フィールド	説明
Routing process “ospf 201” with ID 10.0.0.1	プロセス ID および OSPF ルータ ID。
Supports...	サポートされるサービス タイプの数 (タイプ 0 のみ)

フィールド	説明
SPF schedule delay	SPF 計算の遅延時間（秒単位）。
Minimum LSA interval	リンクステートアドバタイズメント間の最小間隔（秒単位）。
LSA group pacing timer	設定されている LSA グループ ペーシング タイマー（秒単位）。
Interface flood pacing timer	設定されている LSA フラッド ペーシング タイマー（ミリ秒単位）。
Retransmission pacing timer	設定されている LSA 再送信ペーシング タイマー（ミリ秒単位）。
Number of external LSA	外部リンクステートアドバタイズメントの数。
Number of opaque AS LSA	不透明リンクステートアドバタイズメントの数。
Number of DCbitless external and opaque AS LSA	デマンド回線外部および不透明リンクステートアドバタイズメントの数。
Number of DoNotAge external and opaque AS LSA	do not age 外部および不透明リンクステートアドバタイズメントの数。
Number of areas in this router is	ルータに設定されているエリアの数。
External flood list length	外部フラッドリストの長さ。
BFD is enabled	BFD が OSPF プロセスでイネーブルにされています。

次に、Type-5 LSA 機能の OSPF Forwarding Address Suppression が設定されている場合の **show ip ospf** コマンドの出力からの抜粋を示します。

```
Device#show ip ospf
.
.
.
Area 2
  Number of interfaces in this area is 4
  It is a NSSA area
  Perform type-7/type-5 LSA translation, suppress forwarding address
.
.
.
Routing Process "ospf 1" with ID 192.168.0.1
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Initial SPF schedule delay 5000 msec
  Minimum hold time between two consecutive SPF's 10000 msec
  Maximum wait time between two consecutive SPF's 10000 msec
  Incremental-SPF disabled
```

```

Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 126: show ip ospf フィールドの説明

フィールド	説明
Area	OSPF エリアおよびタグ。
Number of interfaces...	エリアで設定されているインターフェイスの数。
It is...	指定できるタイプは、内部、エリア境界、または自律システム境界です。
Routing process “ospf 1” with ID 192.168.0.1	プロセス ID および OSPF ルータ ID。
Supports...	サポートされるサービス タイプの数 (タイプ 0 のみ)
Initial SPF schedule delay	起動時の SPF 計算の遅延時間。
Minimum hold time	連続する SPF 計算間の最小ホールド時間 (ミリ秒単位)。
Maximum wait time	連続する SPF 計算間の最大ホールド時間 (ミリ秒単位)。
Incremental-SPF	増分 SPF 計算のステータス。
Minimum LSA...	リンクステート アドバタイズメント間の最小間隔 (秒単位)、およびリンクステート アドバタイズメント間の最小到着時間 (ミリ秒単位)。
LSA group pacing timer	設定されている LSA グループ ペーシング タイマー (秒単位)。
Interface flood pacing timer	設定されている LSA フラッド ペーシング タイマー (ミリ秒単位)。
Retransmission pacing timer	設定されている LSA 再送信ペーシング タイマー (ミリ秒単位)。
Number of...	受信した LSA の数およびタイプ
Number of external LSA	外部リンクステート アドバタイズメントの数。

フィールド	説明
Number of opaque AS LSA	不透明リンクステートアドバタイズメントの数。
Number of DCbitless external and opaque AS LSA	デマンド回線外部および不透明リンクステートアドバタイズメントの数。
Number of DoNotAge external and opaque AS LSA	do not age 外部および不透明リンクステートアドバタイズメントの数。
Number of areas in this router is	タイプ別にリストされたルータに設定されているエリアの数。
External flood list length	外部フラッドリストの長さ。

次に、**show ip ospf** コマンドの出力例を示します。この例では、ユーザが、**redistribution maximum-prefix** コマンドを使用して再配布ルート of の制限を 2000 に設定しています。SPF スロットリングは **timer throttle spf** コマンドを使用して設定されました。

```
Device#show ip ospf 1
Routing Process "ospf 1" with ID 10.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
It is an autonomous system boundary router
Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
    Threshold for warning message 75%
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 127: show ip ospf フィールドの説明

フィールド	説明
Routing process "ospf 1" with ID 10.0.0.1	プロセス ID および OSPF ルータ ID。
Supports ...	サポートされているサービスのタイプの数。
It is ...	指定できるタイプは、内部、エリア境界、または自律システム境界ルータです。
Redistributing External Routes from	再配布されたルート of のプロトコル別リスト。
Maximum limit of redistributed prefixes	再配布ルート of の数の制限を指定するために redistribution maximum-prefix コマンドに設定されている値。

フィールド	説明
Threshold for warning message	redistributionmaximum-prefix コマンドで設定された、警告メッセージを表示するために必要な再配布ルートのしきい値の割合。デフォルトは、最大値の 75% です。
Initial SPF schedule delay	SPF スロットリングの初期 SPF スケジュールまでの遅延（ミリ秒単位）。 timersthrottlespf コマンドを使用して設定されません。
Minimum hold time between two consecutive SPF's	SPF スロットリングの 2 つの連続する SPF 計算間の最小ホールド時間（ミリ秒単位）。 timersthrottlespf コマンドを使用して設定されます。
Maximum wait time between two consecutive SPF's	SPF スロットリングの 2 つの連続する SPF 計算間の最大ホールド時間（ミリ秒単位）。 timersthrottlespf コマンドを使用して設定されます。
Number of areas	ルータのエリアの数、エリアアドレスなど。

次に、**show ip ospf** コマンドの出力例を示します。この例では、ユーザが、LSA スロットリングを設定しています。これらの出力行は太字で示されます。

```

Device#show ip ospf 1
Routing Process "ospf 4" with ID 10.10.24.4
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Initial SPF schedule delay 5000 msec
  Minimum hold time between two consecutive SPF's 10000 msec
  Maximum wait time between two consecutive SPF's 10000 msec
  Incremental-SPF disabled
Initial LSA throttle delay 100 msec
Minimum hold time for LSA throttle 10000 msec

Maximum wait time for LSA throttle 45000 msec
Minimum LSA arrival 1000 msec
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msec
  Retransmission pacing timer 66 msec
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  External flood list length 0
    Area 24
      Number of interfaces in this area is 2
      Area has no authentication
      SPF algorithm last executed 04:28:18.396 ago
      SPF algorithm executed 8 times
      Area ranges are
      Number of LSA 4. Checksum Sum 0x23EB9
      Number of opaque link LSA 0. Checksum Sum 0x0
      Number of DCbitless LSA 0
      Number of indication LSA 0

```

```
Number of DoNotAge LSA 0
Flood list length 0
```

次に、**show ip ospf** コマンドの例を示します。この例では、ユーザが、**redistribution maximum-prefix** コマンドを使用して再配布ルートの制限を 2000 に設定しています。SPF スロットリングは **timer throttle spf** コマンドを使用して設定されました。

```
Device#show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.0
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
It is an autonomous system boundary router
Redistributing External Routes from,
    static, includes subnets in redistribution
Maximum limit of redistributed prefixes 2000
Threshold for warning message 75%
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 128: show ip ospf フィールドの説明

フィールド	説明
Routing process "ospf 1" with ID 192.168.0.0	プロセス ID および OSPF ルータ ID。
Supports ...	サポートされている TOS の数。
It is ...	指定できるタイプは、内部、エリアボーダーまたは自律システム境界ルータです。
Redistributing External Routes from	再配布されたルートのプロトコル別リスト。
Maximum limit of redistributed prefixes	再配布ルートの数の制限を指定するために redistribution maximum-prefix コマンドに設定されている値。
Threshold for warning message	redistribution maximum-prefix コマンドで設定された、警告メッセージを表示するために必要な再配布ルートのしきい値の割合。デフォルトは、最大値の 75% です。
Initial SPF schedule delay	SPF スロットリングの初期 SPF スケジュールまでの遅延（ミリ秒単位）。 timer throttle spf コマンドを使用して設定されます。
Minimum hold time between two consecutive SPFs	SPF スロットリングの 2 つの連続する SPF 計算間の最小ホールド時間（ミリ秒単位）。 timer throttle spf コマンドを使用して設定されます。

フィールド	説明
Maximum wait time between two consecutive SPFs	SPF スロットリングの2つの連続する SPF 計算間の最大ホールド時間（ミリ秒単位）。 timersthrotlespf コマンドを使用して設定されます。
Number of areas	ルータのエリアの数、エリアアドレスなど。

次に、**show ip ospf** コマンドの出力例を示します。この例では、ユーザが、LSA スロットリングを設定しています。これらの出力行は太字で示されます。

```

Device#show ip ospf 1
Routing Process "ospf 4" with ID 10.10.24.4
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Initial SPF schedule delay 5000 msec
  Minimum hold time between two consecutive SPFs 10000 msec
  Maximum wait time between two consecutive SPFs 10000 msec
  Incremental-SPF disabled
  Initial LSA throttle delay 100 msec
  Minimum hold time for LSA throttle 10000 msec
  Maximum wait time for LSA throttle 45000 msec
  Minimum LSA arrival 1000 msec
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msec
  Retransmission pacing timer 66 msec
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  External flood list length 0
    Area 24
      Number of interfaces in this area is 2
      Area has no authentication
      SPF algorithm last executed 04:28:18.396 ago
      SPF algorithm executed 8 times
      Area ranges are
      Number of LSA 4. Checksum Sum 0x23EB9
      Number of opaque link LSA 0. Checksum Sum 0x0
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0

```

show ip ospf border-routers

エリア境界ルータ（ABR）および自律システム境界ルータ（ASBR）に対する内部 Open Shortest Path First（OSPF）ルーティング テーブル エントリを表示するには、特権 EXEC モードで **show ip ospf border-routers** コマンドを使用します。

show ip ospf border-routers

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**show ip ospf border-routers** コマンドの出力例を示します。

```
Device#show ip ospf border-routers
OSPF Process 109 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 192.168.97.53 [10] via 172.16.1.53, Serial0, ABR, Area 0.0.0.3, SPF 3
i 192.168.103.51 [10] via 192.168.96.51, Serial0, ABR, Area 0.0.0.3, SPF 3
I 192.168.103.52 [22] via 192.168.96.51, Serial0, ASBR, Area 0.0.0.3, SPF 3
I 192.168.103.52 [22] via 172.16.1.53, Serial0, ASBR, Area 0.0.0.3, SPF 3
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 129: show ip ospf border-routers フィールドの説明

フィールド	説明
192.168.97.53	宛先のルータ ID
[10]	このルートを使用するコスト
via 172.16.1.53	宛先に対するネクスト ホップ
Serial0	発信インターフェイスのインターフェイス タイプ
ABR	宛先のルータ タイプ。ABR、ASBR またはこれら両方のいずれかです。
Area	このルートが学習されるエリアのエリア ID。
SPF 3	このルートをインストールする Shortest Path First（SPF）計算の内部番号。

show ip ospf database

特定のルータの Open Shortest Path First (OSPF) データベースに関連する情報リストを表示するには、EXEC モードで **show ip ospf database** コマンドを使用します。

```

show ip ospf [process-id area-id] database
show ip ospf [process-id area-id] database [adv-router [ip-address]]
show ip ospf [process-id area-id] database [asbr-summary] [link-state-id]
show ip ospf [process-id area-id] database [asbr-summary] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [asbr-summary] [link-state-id] [self-originate]
[link-state-id]
show ip ospf [process-id area-id] database [database-summary]
show ip ospf [process-id] database [external] [link-state-id]
show ip ospf [process-id] database [external] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [external] [link-state-id] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [network] [link-state-id]
show ip ospf [process-id area-id] database [network] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [network] [link-state-id] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [nssa-external] [link-state-id]
show ip ospf [process-id area-id] database [nssa-external] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [nssa-external] [link-state-id] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [router] [link-state-id]
show ip ospf [process-id area-id] database [router] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [router] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [summary] [link-state-id]
show ip ospf [process-id area-id] database [summary] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [summary] [link-state-id] [self-originate] [link-state-id]

```

Syntax Description

<i>process-id</i>	(任意) 内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される数は、OSPFルーティングプロセスをイネーブルにするときに管理目的で割り当てられた数です。
<i>area-id</i>	(任意) 特定のエリアを定義するために使用する network ルータ コンフィギュレーション コマンドで定義された OSPF アドレス範囲に関連付けられるエリア番号。
adv-router <i>[ip-address]</i>	(任意) 指定ルータのすべてのLSAを表示します。IPアドレスを指定しない場合、ローカルルータ自体の情報が表示されます (これは self-originate の場合と同じです)。

<i>link-state-id</i>	<p>(任意) アドバタイズメントによって説明されるインターネット環境の部分。入力値は、アドバタイズメントの LS タイプにより異なります。IP アドレス形式で入力する必要があります。</p> <p>リンクステートアドバタイズメントがネットワークを示す場合、<i>link-state-id</i> では、次のいずれかの形式を使用できます。</p> <p>ネットワークの IP アドレス (タイプ 3 サマリー リンク アドバタイズメントおよび自律システム外部リンク アドバタイズメントなどの場合)。</p> <p>リンクステート ID から取得された派生アドレス (ネットワークのサブネット マスクを使用してネットワーク リンク アドバタイズメントのリンクステート ID をマスクすることによって、ネットワークの IP アドレスが生成されることに注意してください)。</p> <p>リンクステートアドバタイズメントにルータの説明が記載されている場合は、必ず、リンクステート ID が、記載されたルータの OSPF ルータ ID になります。</p> <p>自律システム外部アドバタイズメント (LS タイプ=5) がデフォルトのルートを説明する場合、そのリンクステート ID はデフォルトの宛先 (0.0.0.0) に設定されます。</p>
asbr-summary	(任意) 自律システム境界ルータ サマリー LSA 限定の情報を表示します。
database-summary	(任意) データベースの各エリアの各 LSA タイプの数および合計を表示します。
external	(任意) 外部 LSA の情報だけを表示します。
network	(任意) ネットワーク LSA の情報だけを表示します。
nssa-external	(任意) NSSA 外部 LSA の情報だけを表示します。
router	(任意) ルータ LSA の情報だけを表示します。
self-originate	(任意) 自己生成 LSA (ローカルルータから) だけ表示します。
summary	(任意) サマリー LSA の情報だけを表示します。

Command Modes EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、さまざまな形式で、異なる OSPF リンクステート アドバタイズメントに関する情報を提供します。

Examples

次に、引数やキーワードが使用されていないときの `show ip ospf database` コマンドの出力例を示します。

```
Device#show ip ospf database
OSPF Router with id(192.168.239.66) (Process ID 300)
    Displaying Router Link States(Area 0.0.0.0)
  Link ID      ADV Router    Age      Seq#       Checksum    Link count
  172.16.21.6  172.16.21.6  1731    0x80002CFB 0x69BC      8
  172.16.21.5  172.16.21.5  1112    0x800009D2 0xA2B8      5
  172.16.1.2   172.16.1.2   1662    0x80000A98 0x4CB6      9
  172.16.1.1   172.16.1.1   1115    0x800009B6 0x5F2C      1
  172.16.1.5   172.16.1.5   1691    0x80002BC  0x2A1A      5
  172.16.65.6  172.16.65.6  1395    0x80001947 0xEEE1      4
  172.16.241.5 172.16.241.5 1161    0x8000007C 0x7C70      1
  172.16.27.6  172.16.27.6  1723    0x80000548 0x8641      4
  172.16.70.6  172.16.70.6  1485    0x80000B97 0xEB84      6
    Displaying Net Link States(Area 0.0.0.0)
  Link ID      ADV Router    Age      Seq#       Checksum
  172.16.1.3   192.168.239.66 1245    0x800000EC 0x82E
    Displaying Summary Net Link States(Area 0.0.0.0)
  Link ID      ADV Router    Age      Seq#       Checksum
  172.16.240.0 172.16.241.5 1152    0x80000077 0x7A05
  172.16.241.0 172.16.241.5 1152    0x80000070 0xAEB7
  172.16.244.0 172.16.241.5 1152    0x80000071 0x95CB
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 130: show ip ospf Database フィールドの説明

フィールド	説明
Link ID	ルータ ID 番号
ADV Router	アドバタイズ ルータの ID。
Age	リンク ステート経過時間
Seq#	リンク ステート シーケンス番号（以前の、または重複した LSA を検出します）
Checksum	リンクステートアドバタイズメントの詳細な内容の Fletcher チェックサム
Link count	ルータで検出されたインターフェイスの数

次に、`asbr-summary` キーワードを指定した場合の `show ip ospf database` コマンドの出力例を示します。

```
Device#show ip ospf database asbr-summary
OSPF Router with id(192.168.239.66) (Process ID 300)
    Displaying Summary ASB Link States(Area 0.0.0.0)
  LS age: 1463
  Options: (No TOS-capability)
  LS Type: Summary Links(AS Boundary Router)
  Link State ID: 172.16.245.1 (AS Boundary Router address)
  Advertising Router: 172.16.241.5
  LS Seq Number: 80000072
  Checksum: 0x3548
```

```
Length: 28
Network Mask: 0.0.0.0 TOS: 0 Metric: 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 131: show ip ospf database asbr-summary フィールドの説明

フィールド	説明
OSPF Router with id	ルータ ID 番号
Process ID	OSPF プロセス ID
LS age	リンク ステート経過時間
Options	サービス オプションのタイプ (タイプ 0 のみ)
LS Type	リンク ステート タイプ
Link State ID	リンク ステート ID (自律システム境界ルータ)
Advertising Router	アドバタイズルータの ID。
LS Seq Number	リンク ステートシーケンス (以前の、または重複したLSAを検出します)。
Checksum	LS のチェックサム (リンクステート アドバタイズメントの詳細な内容の Fletcher チェックサム)
Length	LSA の長さ (バイト単位)
Network Mask	実行されたネットワーク マスク
TOS	サービスのタイプ。
Metric	リンク ステート メトリック

次に、**external** キーワードを指定した場合の **show ip ospf database** コマンドの出力例を示します。

```
Device#show ip ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)
    Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.105.0.0 (External Network Number)
Advertising Router: 172.16.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 1
    Forward Address: 0.0.0.0
    External Route Tag: 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 132: show ip ospf database external フィールドの説明

フィールド	説明
OSPF Router with id	ルータ ID 番号
Autonomous system	OSPF 自律システム番号 (OSPF プロセス ID)
LS age	リンク ステート経過時間
Options	サービス オプションのタイプ (タイプ 0 のみ)
LS Type	リンク ステート タイプ
Link State ID	リンク ステート ID (外部ネットワーク番号)。
Advertising Router	アドバタイズルータの ID。
LS Seq Number	リンク ステートシーケンス番号 (以前の、または重複した LSA を検出します)
Checksum	LS のチェックサム (LSA の詳細な内容の Fletcher チェックサム)。
Length	LSA の長さ (バイト単位)
Network Mask	実行されたネットワーク マスク
Metric Type	外部タイプ。
TOS	サービスのタイプ。
Metric	リンク ステートメトリック
Forward Address	転送アドレス。アドバタイズされた宛先へのデータトラフィックは、このアドレスに転送されます。転送アドレスが 0.0.0.0 に設定されている場合は、代わりに、データトラフィックがアドバタイズメントの送信元に転送されます。
External Route Tag	外部ルートタグ、各外部ルートに関連付けられる 32 ビットフィールド。これは、OSPF プロトコル自体では使用されません。

次に、**network** キーワードを指定した場合の **show ip ospf database** コマンドの出力例を示します。

```
Device#show ip ospf database network
  OSPF Router with id(192.168.239.66) (Process ID 300)
    Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
```

```

Link State ID: 172.16.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
    Attached Router: 192.168.239.66
    Attached Router: 172.16.241.5
    Attached Router: 172.16.1.1
    Attached Router: 172.16.54.5
    Attached Router: 172.16.1.5

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 133: show ip ospf database network フィールドの説明

フィールド	説明
OSPF Router with id	ルータ ID 番号
Process ID 300	OSPF プロセス ID
LS age	リンク ステート経過時間
Options	サービス オプションのタイプ (タイプ 0 のみ)
LS Type:	リンク ステート タイプ
Link State ID	指定ルータのリンクステート ID
Advertising Router	アドバタイズルータの ID。
LS Seq Number	リンクステートシーケンス (以前の、または重複したLSAを検出します)。
Checksum	LS のチェックサム (リンクステートアドバタイズメントの詳細な内容の Fletcher チェックサム)
Length	LSA の長さ (バイト単位)
Network Mask	実行されたネットワーク マスク
AS Boundary Router	ルータ タイプの定義
Attached Router	ネットワークに関連付けられるルータの IP アドレス別リスト

次に、**router** キーワードを指定した場合の **show ip ospf database** コマンドの出力例を示します。

```

Device#show ip ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Router Link States(Area 0.0.0.0)
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 172.16.21.6
Advertising Router: 172.16.21.6

```

```

LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
155   Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 172.16.21.5
(Link Data) Router Interface address: 172.16.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 134: show ip ospf database router フィールドの説明

フィールド	説明
OSPF Router with id	ルータ ID 番号
Process ID	OSPF プロセス ID
LS age	リンク ステート経過時間
Options	サービス オプションのタイプ (タイプ 0 のみ)
LS Type	リンク ステート タイプ
Link State ID	リンクステート ID
Advertising Router	アドバタイズルータの ID。
LS Seq Number	リンクステートシーケンス (以前の、または重複したLSAを検出します)。
Checksum	LS のチェックサム (リンクステート アドバタイズメントの詳細な内容の Fletcher チェックサム)
Length	LSA の長さ (バイト単位)
AS Boundary Router	ルータ タイプの定義
Number of Links	アクティブ リンクの数
link ID	リンク タイプ
Link Data	ルータ インターフェイス アドレス
TOS	タイプ オブ サービス メトリック (タイプ 0 限定)

次に、**summary** キーワードを指定した場合の **show ip ospf database** コマンドの出力例を示します。

```

Device#show ip ospf database summary
      OSPF Router with id(192.168.239.66) (Process ID 300)
          Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401

```

```
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 172.16.240.0 (summary Network Number)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 135: show ip ospf database summary フィールドの説明

フィールド	説明
OSPF Router with id	ルータ ID 番号
Process ID	OSPF プロセス ID
LS age	リンク ステート経過時間
Options	サービス オプションのタイプ (タイプ 0 のみ)
LS Type	リンク ステート タイプ
Link State ID	リンク ステート ID (サマリー ネットワーク番号)。
Advertising Router	アドバタイズルータの ID。
LS Seq Number	リンク ステートシーケンス (以前の、または重複した LSA を検出します)。
Checksum	LS のチェックサム (リンクステート アドバタイズメントの詳細な内容の Fletcher チェックサム)
Length	LSA の長さ (バイト単位)
Network Mask	実行されたネットワーク マスク
TOS	サービスのタイプ。
Metric	リンク ステート メトリック

次に、**database-summary** キーワードを指定した場合の **show ip ospf database** コマンドの出力例を示します。

```
Device#show ip ospf database database-summary
OSPF Router with ID (10.0.0.1) (Process ID 1)
Area 0 database summary
  LSA Type      Count  Delete  Maxage
  Router        3      0        0
  Network       0      0        0
  Summary Net   0      0        0
  Summary ASBR  0      0        0
  Type-7 Ext    0      0        0
  Self-originated Type-7  0
  Opaque Link   0      0        0
```

```

    Opaque Area    0        0        0
    Subtotal      3        0        0
Process 1 database summary
LSA Type          Count    Delete  Maxage
Router            3        0        0
Network           0        0        0
Summary Net       0        0        0
Summary ASBR     0        0        0
Type-7 Ext        0        0        0
Opaque Link       0        0        0
Opaque Area       0        0        0
Type-5 Ext        0        0        0
    Self-originated Type-5  200
Opaque AS         0        0        0
Total             203       0        0

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 136: show ip ospf database database-summary フィールドの説明

フィールド	説明
Area 0 database summary	エリア番号
Count	最初のカラムで特定されたタイプの LSA の数
Router	エリアのルータ LSA の数
Network	エリアのネットワーク LSA の数
Summary Net	エリアの要約 LSA の数
Summary ASBR	エリアの要約自律システム境界ルータ (ASBR) リンクステートアドバタイズメントの数
Type-7 Ext	タイプ 7 LSA の数
Self-originated Type-7	自動送信タイプ 7 LSA
Opaque Link	タイプ 9 LSA の数
Opaque Area	タイプ 10 LSA カウント
Subtotal	エリアの LSA の合計
Delete	エリア内で「Deleted」とマークされたリンク ステート アドバタイズメントの数。
Maxage	エリア内で「Maxaged」とマークされたリンク ステート アドバタイズメントの数。
Process 1 database summary	プロセスのデータベース サマリー
Count	最初のカラムで特定されたタイプの LSA の数

フィールド	説明
Router	プロセスのルータ LSA の数
Network	プロセスのネットワーク LSA の数
Summary Net	プロセスのサマリー LSA の数
Summary ASBR	プロセスの要約自律システム境界ルータ (ASBR) リンクステートアドバタイズメントの数
Type-7 Ext	タイプ 7 LSA の数
Opaque Link	タイプ 9 LSA の数
Opaque Area	タイプ 10 LSA の数
Type-5 Ext	タイプ 5 LSA の数
Self-Originated Type-5	自動送信タイプ 5 LSA の数
Opaque AS	タイプ 11 LSA の数
Total	プロセスの LSA の合計
Delete	プロセス内で「Deleted」とマークされたリンク ステートアドバタイズメントの数。
Maxage	プロセス内で「Maxaged」とマークされたリンク ステートアドバタイズメントの数。

show ip ospf interface

Open Shortest Path First (OSPF) に関連するインターフェイス情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ip ospf interface** コマンドを使用します。

show ip [ospf] [process-id] interface [type number] [brief] [multicast] [topology {topology-name | base}]

Syntax Description

<i>process-id</i>	(任意) プロセス ID 番号。この引数を指定すると、指定されたルーティングプロセスの情報だけが追加されます。指定できる範囲は 1 ~ 65535 です。
<i>type</i>	(任意) インターフェイスタイプ。引数 <i>type</i> を指定すると、指定されたインターフェイスタイプの情報だけが追加されます。
<i>number</i>	(任意) インターフェイス番号。引数 <i>number</i> を指定すると、指定されたインターフェイス番号の情報だけが追加されます。
brief	(任意) OSPF インターフェイス、状態、アドレスとマスク、およびデバイスのエリアに関する簡単な概要情報を表示します。
multicast	(任意) マルチキャスト情報を表示します。
topology topology-name	(任意) ネームドトポロジインスタンスに関する OSPF 関連情報を表示します。
topology base	(任意) 基本トポロジに関する OSPF 関連情報を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、イーサネット インターフェイス 0/0 が指定されている場合の **show ip ospf interface** コマンドの出力例を示します。

```
Device#show ip ospf interface ethernet 0/0

Ethernet0/0 is up, line protocol is up
 Internet Address 192.168.254.202/24, Area 0
 Process ID 1, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 10
 Topology-MTID Cost Disabled Shutdown Topology Name
    0          10      no      no      Base
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.99.1, Interface address 192.168.254.202
```

```

Backup Designated router (ID) 192.168.254.10, Interface address 192.168.254.10
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.254.10 (Backup Designated Router)
Suppress hello for 0 neighbor(s)

```

Cisco IOS リリース 12.2(33)SRB では、次の **show ip ospf interface brief topology VOICE** コマンドの出力例には、Multitopology Routing (MTR) VOICE トポロジがインターフェイスコンフィギュレーションで設定されていることなどの、情報の概要が示されます。

```
Device#show ip ospf interface brief topology VOICE
```

```

VOICE Topology (MTID 10)
Interface    PID   Area           IP Address/Mask    Cost   State Nbrs F/C
Lo0          1     0              10.0.0.2/32        1     LOOP  0/0
Se2/0       1     0              10.1.0.2/30        10    P2P   1/1

```

次の **show ip ospf interface brief topology VOICE** コマンドの出力例では、インターフェイスに対する MTR VOICE トポロジの詳細が示されています。キーワード **brief** を指定せずにこのコマンドを入力すると、詳細が表示されます。

```
Device#show ip ospf interface topology VOICE
```

```

                VOICE Topology (MTID 10)
Loopback0 is up, line protocol is up
  Internet Address 10.0.0.2/32, Area 0
  Process ID 1, Router ID 10.0.0.2, Network Type LOOPBACK
Topology-MTID    Cost    Disabled  Shutdown  Topology Name
   10             1       no        no        VOICE
Loopback interface is treated as a stub
Host Serial2/0 is up, line protocol is up
  Internet Address 10.1.0.2/30, Area 0
  Process ID 1, Router ID 10.0.0.2, Network Type POINT_TO_POINT
Topology-MTID    Cost    Disabled  Shutdown  Topology Name
   10             10      no        no        VOICE
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.0.0.1
Suppress hello for 0 neighbor(s)

```

Cisco IOS リリース 12.2(33)SRC では、次の **show ip ospf interface** コマンドの出力例は、設定された存続可能時間 (TTL) の制限に関する詳細を表示します。

```

Device#show ip ospf interface ethernet 0
.
.
.
Strict TTL checking enabled
! or a message similar to the following is displayed
Strict TTL checking enabled, up to 4 hops allowed
.
.
.

```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 137: show ip ospf interface フィールドの説明

フィールド	説明
Ethernet	物理リンクのステータス、およびプロトコルの動作ステータス。
Process ID	OSPF プロセス ID
Area	OSPF エリア。
Cost	インターフェイスに割り当てられる管理コスト。
State	インターフェイスの動作状態。
Nbrs F/C	OSPF ネイバー カウント。
Internet Address	インターフェイス IP アドレス、サブネットマスク、およびエリアアドレス。
Topology-MTID	MTR トポロジの Multitopology Identifier (MTID)。ピアに送信する情報が関連付けられるトポロジをプロトコルが識別できるように割り当てられている番号。
Transmit Delay	転送遅延 (秒単位)、インターフェイス ステート、およびデバイス プライオリティ。
Designated Router	指定ルータ ID および各インターフェイス IP アドレス。
Backup Designated router	バックアップ指定ルータ ID および各インターフェイス IP アドレス。
Timer intervals configured	タイマーインターバルの設定。
Hello	次の hello パケットがこのインターフェイスから送信されるまでの時間 (秒単位)。
Strict TTL checking enabled	使用できるホップは 1 つだけです。
Strict TTL checking enabled, up to 4 hops allowed	一定のホップ カウントが明示的に設定されています。

フィールド	説明
Neighbor Count	ネットワーク ネイバーの数、および隣接ネイバーのリスト。

show ip ospf neighbor

Open Shortest Path First (OSPF) ネイバー情報をインターフェイス単位で表示するには、特権 EXEC モードで **show ip ospf neighbor** コマンドを使用します。

show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**] [**summary**] [**per-instance**]

Syntax Description

<i>interface-type</i> <i>interface-number</i>	(任意) 特定の OSPF インターフェイスに関連付けられるタイプおよび番号。
<i>neighbor-id</i>	(任意) ネイバー ホスト名または A.B.C.D 形式の IP アドレス。
detail	(任意) 指定されたすべてのネイバーの詳細を表示します (すべてのネイバーをリストします)。
summary	(任意) すべてのネイバーの総数サマリーを表示します。
per-instance	(任意) 各ネイバー状態のネイバーの総数を表示します。設定された OSPF インスタンスごとに出力が個別に出力されます。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の **show ip ospf neighbor** コマンドの出力例では、各ネイバーのサマリー情報が 1 行に表示されています。

```
Device#show ip ospf neighbor
```

```
Neighbor ID  Pri  State           Dead Time   Address           Interface
10.199.199.137 1    FULL/DR       0:00:31    192.168.80.37    Ethernet0
172.16.48.1    1    FULL/DROTHER  0:00:33    172.16.48.1     Fddi0
172.16.48.200 1    FULL/DROTHER  0:00:33    172.16.48.200   Fddi0
10.199.199.137 5    FULL/DR       0:00:33    172.16.48.189   Fddi0
```

次に、ネイバー ID と一致するネイバーに関するサマリー情報を示す出力例を示します。

```
Device#show ip ospf neighbor 10.199.199.137
```

```
Neighbor 10.199.199.137, interface address 192.168.80.37
  In the area 0.0.0.0 via interface Ethernet0
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:04
Neighbor 10.199.199.137, interface address 172.16.48.189
  In the area 0.0.0.0 via interface Fddi0
```

```
Neighbor priority is 5, State is FULL
Options 2
Dead timer due in 0:00:32
Link State retransmission due in 0:00:03
```

インターフェイスとネイバー ID を指定すると、次に示す出力例のように、インターフェイスのネイバー ID と一致するネイバーが表示されます。

```
Device#show ip ospf neighbor ethernet 0 10.199.199.137

Neighbor 10.199.199.137, interface address 192.168.80.37
  In the area 0.0.0.0 via interface Ethernet0
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:37
  Link State retransmission due in 0:00:04
```

また、次に示す出力例のように、ネイバー ID なしでインターフェイスを指定して、指定したインターフェイスのすべてのネイバーを表示することもできます。

```
Device#show ip ospf neighbor fddi 0

      ID          Pri   State           Dead Time      Address         Interface
172.16.48.1      1    FULL/DROTHER    0:00:33       172.16.48.1    Fddi0
172.16.48.200   1    FULL/DROTHER    0:00:32       172.16.48.200  Fddi0
10.199.199.137  5    FULL/DR         0:00:32       172.16.48.189  Fddi0
```

次に、**show ip ospf neighbor detail** コマンドの出力例を示します。

```
Device#show ip ospf neighbor detail

Neighbor 192.168.5.2, interface address 10.225.200.28
  In the area 0 via interface GigabitEthernet1/0/0
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.225.200.28 BDR is 10.225.200.30
  Options is 0x42
  LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
  Dead timer due in 00:00:36
  Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 138: show ip ospf neighbor detail フィールドの説明

フィールド	説明
Neighbor	ネイバー ルータ ID。
interface address	インターフェイスの IP アドレス。
In the area	OSPF ネイバーが認識されるエリアおよびインターフェイス。

フィールド	説明
Neighbor priority	ネイバーおよびネイバー状態のルータ プライオリティ。
State	OSPF ステート一方の OSPF ネイバーが TTL セキュリティをイネーブルにしている場合、接続のもう一方は、INIT 状態のネイバーを示します。
state changes	ネイバーが作成されて以降の状態変化の数。この値は、 clearipospfcountersneighbor コマンドを使用してリセットできます。
DR is	インターフェイスの指定ルータのルータ ID
BDR is	インターフェイスのバックアップ指定ルータのルータ ID
Options	hello packet options フィールドの内容 (E ビット専用。可能な値は 0 および 2 です。2 はエリアがスタブでないことを示し、0 はエリアがスタブであることを示します)。
LLS Options..., last OOB-Resync	時:分:秒形式で指定される時刻前に実行されたリンクローカルシグナリングおよびアウトオブバンド (OOB) リンクステートデータベース再同期。これは、ノンストップフォワーディング (NSF) 情報です。このフィールドは、最後に成功した NSF 対応ルータとのアウトオブバンド再同期化を示します。
Dead timer due in	Cisco IOS ソフトウェアがネイバー デッドを宣言するまでの予想時間 (時:分:秒形式)。
Neighbor is up for	ネイバーが二方向状態になってからの時間 (時:分:秒形式)。
Index	エリア規模および自律システム規模の再送信キューのネイバーの位置。
retransmission queue length	再送信キューのエレメントの数
number of retransmission	アップデート パケットがフラッディング中に再送信された回数。
First	フラッディング詳細のメモリ位置。
Next	フラッディング詳細のメモリ位置。
Last retransmission scan length	最後の再送信パケット内のリンクステート アドバタイズメント (LSA) の数
maximum	任意の再送信パケットで送信された LSA の最大数
Last retransmission scan time	最後の再送信パケットの構築にかかった時間。
maximum	任意の再送信パケットの構築にかかった最大時間 (ミリ秒単位)。

次に、各ネイバーのサマリー情報を1行に表示する **show ip ospf neighbor** コマンドの出力例を示します。一方の OSPF ネイバーが TTL セキュリティをイネーブルにしている場合、接続のもう一方は、INIT 状態のネイバーを示します。

```
Device#show ip ospf neighbor

Neighbor ID    Pri   State           Dead Time   Address           Interface
10.199.199.137 1     FULL/DR         0:00:31    192.168.80.37    Ethernet0
172.16.48.1    1     FULL/DROTHER    0:00:33    172.16.48.1      Fddi0
172.16.48.200 1     FULL/DROTHER    0:00:33    172.16.48.200    Fddi0
10.199.199.137 5     FULL/DR         0:00:33    172.16.48.189    Fddi0
172.16.1.201  1     INIT/DROTHER    00.00.35   10.1.1.201        Ethernet0/0
```

Cisco IOS Release 15.1(3)S

次の **show ip ospf neighbor** コマンドの出力例は、ネイバーの視点からネットワークを示しています。

```
Device#show ip ospf neighbor 192.0.2.1
      OSPF Router with ID (192.1.1.1) (Process ID 1)

          Area with ID (0)

Neighbor with Router ID 192.0.2.1:
  Reachable over:
    Ethernet0/0, IP address 192.0.2.1, cost 10

  SPF was executed 1 times, distance to computing router 10

  Router distance table:
    192.1.1.1   i   [10]
    192.0.2.1   i   [0]
    192.3.3.3   i   [10]
    192.4.4.4   i   [20]
    192.5.5.5   i   [20]

  Network LSA distance table:
    192.2.12.2   i   [10]
    192.2.13.3   i   [20]
    192.2.14.4   i   [20]
    192.2.15.5   i   [20]
```

次に、**show ip ospf neighbor summary** コマンドの出力例を示します。

```
Device#show ip ospf neighbor summary

Neighbor summary for all OSPF processes

DOWN          0
ATTEMPT       0
INIT          0
2WAY          0
EXSTART       0
EXCHANGE      0
LOADING       0
FULL          1
Total count   1      (Undergoing NSF 0)
```

次に、**show ip ospf neighbor summary per-instance** コマンドの出力例を示します。

```
Device#show ip ospf neighbor summary

      OSPF Router with ID (1.0.0.10) (Process ID 1)

DOWN          0
ATTEMPT       0
INIT          0
2WAY          0
EXSTART       0
EXCHANGE      0
LOADING       0
FULL          1
Total count   1      (Undergoing NSF 0)

Neighbor summary for all OSPF processes

DOWN          0
ATTEMPT       0
INIT          0
2WAY          0
EXSTART       0
EXCHANGE      0
LOADING       0
FULL          1
Total count   1      (Undergoing NSF 0)
```

Table 139: show ip ospf neighbor summary および show ip ospf neighbor summary per-instance のフィールドの説明

フィールド	説明
DOWN	当該ネイバーから情報 (hello) を受信していませんが、この状態でも、そのネイバーに hello パケットを送信することは可能です。
ATTEMPT	この状態は、Non-Broadcast Multi-Access (NBMA) 環境内の手動で設定されたネイバーに対してのみ有効です。Attempt ステートでは、ルータは、デッド時間間隔内に hello を受信しなかったネイバーにポーリング時間間隔ごとにユニキャスト hello パケットを送信します。
INIT	この状態は、ルータがネイバーから受信した hello パケットに、受信側ルータの ID が含まれていなかったことを意味します。ルータがネイバーから hello パケットを受信すると、有効な hello パケットを受信した確認として、送信側のルータ ID を hello パケットにリストします。
2WAY	このネイバー状態は、ルータ間で双方向通信が確立されていることを意味します。
EXSTART	この状態は、2つの隣接ルータ間の隣接関係を作成する最初のステップです。このステップの目標は、どのルータがアクティブであるかを決定し、最初の DD シーケンス番号を決定することです。この状態以上のネイバーの会話は、隣接関係と呼ばれます。

フィールド	説明
EXCHANGE	<p>この状態では、OSPF ルータが Database Descriptor (DBD) パケットを交換します。Database Descriptor にはリンクステートアドバタイズメント (LSA) ヘッダーだけが含まれ、リンクステートデータベース全体のコンテンツが記述されます。各 DBD パケットにはシーケンス番号があり、そのシーケンス番号を増分するのは、セカンダリルータによって明示的に確認されているアクティブルータだけです。また、このステートで、ルータはリンクステート要求パケットとリンクステートアップデートパケット (LSA 全体を含む) を送信します。受信した DBD の内容は、ルータリンクステートデータベースに含まれる情報と比較され、ネイバーに新規または最新のリンクステート情報があるかどうかチェックされます。</p>
LOADING	<p>この状態では、リンクステート情報の実際の交換が行われます。DBD からの情報に基づいて、ルータはリンクステート要求パケットを送信します。次に、ネイバーは、リンクステートアップデートパケットで要求されたリンクステート情報を提供します。隣接中に、デバイスは古い LSA または不足している LSA を受信すると、リンクステート要求パケットを送信してその LSA を要求します。すべてのリンクステートアップデートパケットが確認されます。</p>
FULL	<p>この状態では、デバイスは互いに完全隣接ネイバーとなっています。すべてのデバイスおよびネットワーク LSA が交換され、デバイスのデータベースは完全に同期化されます。</p> <p>Full は、OSPF デバイスの通常のステートです。デバイスが別の状態でスタックしている場合は、隣接関係の形成に問題があることを示しています。唯一の例外は、2-way ステートです。2-way ステートは、ブロードキャストネットワークでは通常です。デバイスは、DR および BDR だけで Full ステートに達します。ネイバーは、常に互いを 2-way と見なします。</p>

show ip ospf virtual-links

Open Shortest Path First (OSPF) 仮想リンクのパラメータと現在の状態を表示するには、EXEC モードで **show ip ospf virtual-links** コマンドを使用します。

show ip ospf virtual-links

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show ip ospf virtual-links コマンドで表示される情報は、OSPF ルーティング操作のデバッグに役立ちます。

Examples

次に、**show ip ospf virtual-links** コマンドの出力例を示します。

```
Device#show ip ospf virtual-links
Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 140: show ip ospf virtual-links フィールドの説明

フィールド	説明
Virtual Link to router 192.168.101.2 is up	OSPF ネイバー、およびそのネイバーとのリンクがアップまたはダウン状態であるか指定します。
Transit area 0.0.0.1	仮想リンクが形成される移行エリア。
via interface Ethernet0	仮想リンクが形成されるインターフェイス。
Cost of using 10	仮想リンクを介して OSPF ネイバーに到達するときのコスト。
Transmit Delay is 1 sec	仮想リンクの移行遅延（秒単位）。
State POINT_TO_POINT	OSPF ネイバーの状態。
Timer intervals...	リンクに設定されるさまざまなタイマー間隔。

フィールド	説明
Hello due in 0:00:08	ネイバーからの次の hello の予想時間。
Adjacency State FULL	ネイバー間の隣接状態。

summary-address (OSPF)

Open Shortest Path First (OSPF) の集約アドレスを作成するには、ルータ コンフィギュレーション モードで **summary-address** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

summary-address **command** **summary-address** {*ip-address mask* | *prefix mask*} [**not-advertise**] [**tag tag**] [**nssa-only**]

no summary-address {*ip-address mask* | *prefix mask*} [**not-advertise**] [**tag tag**] [**nssa-only**]

Syntax Description

<i>ip-address</i>	アドレスの範囲を表すために指定するサマリーアドレス。
<i>mask</i>	サマリールートに使用される IP サブネットマスク。
<i>prefix</i>	宛先の IP ルート プレフィックス。
not-advertise	(任意) 指定されたプレフィックス/マスクペアと一致するルートを抑制します。このキーワードは OSPF だけに適用されます。
tag tag	(任意) ルートマップを介した再配布を制御する「一致」値として使用できるタグ値を指定します。このキーワードは OSPF だけに適用されます。
nssa-only	(任意) 指定したプレフィックスに対して生成されるサマリールートがある場合、そのサマリールートの nssa-only 属性を設定します。これにより、サマリーが Not-So-Stubby-Area (NSSA) エリアに制限されます。

Command Default

このコマンドの動作は、デフォルトではディセーブルです。

Command Modes

ルータ コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

他のルーティングプロトコルから学習したルートを集約できます。サマリーのアドバタイズに使用されるメトリックは、すべての特定ルートの中で最小のメトリックです。このコマンドは、ルーティングテーブルの容量縮小に有効です。

このコマンドを OSPF に対して使用すると、OSPF 自律システム境界ルータ (ASBR) により、このアドレスの対象となる再配布されるすべてのルートの集約として、1つの外部ルートがアドバタイズされます。OSPF の場合、このコマンドでは、OSPF 内に再配布される他のルーティングプロトコルからのルートだけが集約されます。OSPF エリア間のルート集約には **area range** コマンドを使用します。

OSPF は **summary-address 0.0.0.0 0.0.0.0** コマンドをサポートしていません。

Examples

次の例では、集約アドレス 10.1.0.0 にアドレス 10.1.1.0、10.1.2.0、10.1.3.0 などが含まれています。外部 LSA では、アドレス 10.1.0.0 だけがアドバタイズされます。

```
Device(config)#summary-address 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
area range	エリア境界でルートを統合および集約します。
ip ospf authentication-key	OSPF の単純パスワード認証を使用しているネイバー ルータが使用するパスワードを割り当てます。
ip ospf message-digest-key	OSPF Message Digest 5 (MD5) 認証をイネーブルにします。

timers throttle spf

Open Shortest Path First (OSPF) 最短パス優先 (SPF) スロットリングをオンにするには、適切なコンフィギュレーション モードで **timers throttle spf** コマンドを使用します。OSPF SPF スロットリングをオフにするには、このコマンドの **no** 形式を使用します。

timers throttle spf *spf-start spf-hold spf-max-wait*
no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

<i>spf-start</i>	変更後の SPF 計算をスケジューリングするための初期遅延 (ミリ秒単位)。値の範囲は 1 ~ 600000 です。IPv6 の OSPF では、デフォルト値は 5000 です。
<i>spf-hold</i>	2 つの連続する SPF 計算の間の最小ホールド時間 (ミリ秒単位)。値の範囲は 1 ~ 600000 です。IPv6 の OSPF では、デフォルト値は 10,000 です。
<i>spf-max-wait</i>	2 つの連続する SPF 計算の間の最大待機時間 (ミリ秒単位)。値の範囲は 1 ~ 600000 です。IPv6 の OSPF では、デフォルト値は 10,000 です。

Command Default

SPF スロットリングは設定されていません。

Command Modes

IPv6 ルータ コンフィギュレーション (config-rtr) 用のアドレス ファミリ コンフィギュレーション (config-router-af) ルータ アドレス ファミリ トポロジ コンフィギュレーション (config-router-af-topology) ルータ コンフィギュレーション (config-router) OSPF

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

SPF 計算間の初回待機時間は、*spf-start* 引数で指定される時間 (ミリ秒単位) です。連続する各待機間隔は、待機時間が引数 *spf-max-wait* で指定した最大時間 (ミリ秒単位) に達するまで、現在のホールドレベル (ミリ秒単位) の 2 倍となります。値がリセットされるまで、または SPF 計算間でリンクステート アドバタイズメント (LSA) が受信されるまで、従属待機時間は最大のまま残ります。

Release 12.2(33)SRB

マルチトポロジルーティング (MTR) 機能を使用する予定の場合は、この OSPF ルータ コンフィギュレーション コマンドをトポロジ対応にするために、ルータ アドレス ファミリ トポロジ コンフィギュレーション モードで **timers throttle spf** コマンドを実行する必要があります。

Release 15.2(1)T

OSPFv3 プロセスに接続されたインターフェイスで **ospfv3 network manet** コマンドを設定すると、*spf-start*、*spf-hold*、および *spf-max-wait* 引数のデフォルト値は、それぞれ 1000 ミリ秒、1000 ミリ秒、および 2000 ミリ秒に短縮されます。

Examples

次に、**timers throttle spf** コマンドの遅延、ホールド、および最大間隔の各値がそれぞれ 5、1000、および 90,000 ミリ秒に設定されるようにルータを設定する例を示します。

```
router ospf 1
router-id 10.10.10.2
log-adjacency-changes
timers throttle spf 5 1000 90000
redistribute static subnets
network 10.21.21.0 0.0.0.255 area 0
network 10.22.22.0 0.0.0.255 area 00
```

次に、**timers throttle spf** コマンドの遅延、ホールド、および最大間隔の各値がそれぞれ 500、1000、および 10,000 ミリ秒に設定されるように IPv6 を使用したルータを設定する例を示します。

```
ipv6 router ospf 1
event-log size 10000 one-shot
log-adjacency-changes
timers throttle spf 500 1000 10000
```

Related Commands

Command	Description
ospfv3 network manet	ネットワーク タイプをモバイルアドホック ネットワーク (MANET) に設定します。



PART **X**

セキュリティ

• [セキュリティ](#), on page 1367



セキュリティ

- [aaa accounting, on page 1370](#)
- [aaa accounting dot1x, on page 1374](#)
- [aaa accounting identity, on page 1376](#)
- [aaa authentication dot1x, on page 1378](#)
- [aaa new-model, on page 1379](#)
- [authentication host-mode, on page 1381](#)
- [authentication logging verbose, on page 1383](#)
- [authentication mac-move permit, on page 1384](#)
- [authentication priority, on page 1386](#)
- [authentication violation, on page 1389](#)
- [cisp enable, on page 1391](#)
- [clear errdisable interface vlan, on page 1393](#)
- [clear mac address-table, on page 1394](#)
- [confidentiality-offset, on page 1396](#)
- [crypto pki trustpool import, on page 1397](#)
- [debug aaa dead-criteria transaction, on page 1400](#)
- [debug umbrella, on page 1402](#)
- [delay-protection, on page 1403](#)
- [deny \(MAC アクセス リスト コンフィギュレーション\) , on page 1404](#)
- [device-role \(IPv6 スヌーピング\) , on page 1408](#)
- [device-role \(IPv6 ND インспекション\) , on page 1409](#)
- [device-tracking \(インターフェイス コンフィギュレーション\) , on page 1410](#)
- [device-tracking \(VLAN コンフィギュレーション\) , on page 1414](#)
- [device-tracking binding, on page 1417](#)
- [device-tracking logging, on page 1440](#)
- [device-tracking policy, on page 1444](#)
- [device-tracking tracking, on page 1460](#)
- [device-tracking upgrade-cli, on page 1466](#)
- [dnsCrypt \(パラメータマップ\) , on page 1469](#)
- [dot1x critical \(グローバル コンフィギュレーション\) , on page 1470](#)
- [dot1x logging verbose, on page 1471](#)
- [dot1x pae, on page 1472](#)

- dot1x supplicant controlled transient, on page 1473
- dot1x supplicant force-multicast, on page 1474
- dot1x test eapol-capable, on page 1475
- dot1x test timeout, on page 1476
- dot1x timeout, on page 1477
- dtls, on page 1480
- enable password, on page 1482
- enable secret, on page 1485
- epm access-control open, on page 1489
- include-icv-indicator, on page 1490
- ip access-list, on page 1491
- ip access-list role-based, on page 1494
- ip admission, on page 1495
- ip admission name, on page 1496
- ip dhcp snooping database, on page 1499
- ip dhcp snooping information option format remote-id, on page 1501
- ip dhcp snooping verify no-relay-agent-address, on page 1502
- ip http access-class, on page 1503
- ip radius source-interface, on page 1505
- ip source binding, on page 1507
- ip ssh source-interface, on page 1508
- ip verify source, on page 1509
- ipv6 access-list, on page 1511
- ipv6 snooping policy, on page 1513
- key chain macsec, on page 1514
- key config-key password-encrypt, on page 1515
- key-server, on page 1518
- limit address-count, on page 1520
- local-domain (パラメータマップ) , on page 1521
- mab logging verbose, on page 1522
- mab request format attribute 32, on page 1523
- macsec-cipher-suite, on page 1525
- macsec network-link, on page 1527
- match (アクセス マップ コンフィギュレーション) , on page 1528
- mka pre-shared-key, on page 1530
- mka suppress syslogs sak-rekey, on page 1531
- parameter-map type regex, on page 1532
- parameter-map type umbrella global, on page 1536
- password encryption aes, on page 1537
- pattern (パラメータマップ) , on page 1540
- permit (MAC アクセス リスト コンフィギュレーション) , on page 1543
- protocol (IPv6 スヌーピング) , on page 1547
- radius server, on page 1549
- radius-server dead-criteria, on page 1551
- radius-server deadtime, on page 1553

- radius-server directed-request, on page 1555
- radius-server domain-stripping, on page 1558
- sak-rekey, on page 1562
- security level (IPv6 スヌーピング) , on page 1564
- send-secure-announcements, on page 1565
- server-private (RADIUS) , on page 1567
- server-private (TACACS+) , on page 1570
- show aaa clients, on page 1572
- show aaa command handler, on page 1573
- show aaa dead-criteria, on page 1574
- **show aaa local**, on page 1576
- show aaa servers, on page 1578
- show aaa sessions, on page 1579
- show authentication brief, on page 1580
- show authentication sessions, on page 1583
- show cisp, on page 1586
- show dot1x, on page 1588
- show eap pac peer, on page 1590
- show ip access-lists, on page 1591
- show ip dhcp snooping statistics, on page 1594
- show platform software dns-umbrella statistics, on page 1597
- show platform software umbrella switch F0, on page 1598
- show radius server-group, on page 1600
- show tech-support acl, on page 1602
- show tech-support identity, on page 1607
- show umbrella, on page 1616
- show vlan access-map, on page 1618
- show vlan filter, on page 1619
- show vlan group, on page 1620
- ssci-based-on-sci, on page 1621
- switchport port-security aging, on page 1623
- switchport port-security mac-address, on page 1625
- switchport port-security maximum, on page 1628
- switchport port-security violation, on page 1630
- tacacs server, on page 1632
- token (パラメータマップ) , on page 1634
- tracking (IPv6 スヌーピング) , on page 1635
- trusted-port, on page 1637
- umbrella, on page 1638
- use-updated-eth-header, on page 1640
- username, on page 1642
- vlan access-map, on page 1648
- vlan dot1Q tag native, on page 1650
- vlan filter, on page 1651
- vlan group, on page 1652

aaa accounting

RADIUS または TACACS+ を使用する場合に、課金やセキュリティ目的で、要求されたサービスの認証、許可、およびアカウントिंग（AAA）アカウントングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。AAA アカウントングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
no aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
```

Syntax Description

auth-proxy	すべての認証済みプロキシユーザイベントに関する情報を出力します。
system	リロードなどのユーザに関連付けられていないシステムレベルのすべてのイベントのアカウントングを実行します。
network	ネットワークに関連するあらゆるサービス要求にアカウントングを実行します。
exec	EXEC シェルセッションのアカウントングを実行します。このキーワードは、 autocommand コマンドによって生成される情報などのユーザプロファイル情報を返すことができます。
connection	ネットワーク アクセス サーバから確立されたすべてのアウトバウンド接続に関する情報を提供します。
commands level	指定した特権レベルですべてのコマンドのアカウントングを実行します。有効な特権レベル エントリは 0 ~ 15 の整数です。
default	この引数のあとにリストされるアカウントング方式を、アカウントングサービスのデフォルトリストとして使用します。
<i>list-name</i>	次に記載されているアカウントング方式のうち、少なくとも 1 つを含むリストの名前を付けるために使用する文字列です：
start-stop	プロセスの開始時に "start" accounting 通知を送信し、プロセスの終了時に "stop" accounting 通知を送信します。"start" アカウントングレコードはバックグラウンドで送信されます。要求されたユーザプロセスは、"start" accounting 通知がアカウントングサーバで受信されたかどうかに関係なく開始されます。
stop-only	要求されたユーザ プロセスの終了時に、"stop" アカウントング通知を送信します。
none	この回線またはインターフェイスでアカウントングサービスをディセーブルにします。

broadcast (任意) 複数の AAA サーバへのアカウントレコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウントレコードを同時に送信します。最初のサーバが使用できない場合、そのグループ内で定義されたバックアップサーバを使用してフェールオーバーが発生します。

group 「AAA アカウンティングの方式」に記述されているキーワードの 1 つ以上を使用します。
groupname

Command Default

AAA アカウンティングはディセーブルです。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

アカウントを有効にし、回線別またはインターフェイス別に特定のアカウント方式を定義する名前付き方法リストを作成するには、**aaa accounting** コマンドを使用します。

Table 141: AAA アカウンティング方式

キーワード	説明
group radius	aaa group server radius コマンドで定義されるすべての RADIUS サーバのリストを認証に使用します。
group tacacs+	aaa group server tacacs+ コマンドで定義されるすべての TACACS+ サーバのリストを認証に使用します。
group group-name	<i>group-name</i> サーバグループで定義したように、アカウントのための RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

「AAA アカウンティングの方式」の表では、**group radius** 方式および **group tacacs+** 方式は、以前に定義した一連の RADIUS サーバまたは TACACS+ サーバを参照します。ホストサーバを設定するには、**radius server** および **tacacs server** コマンドを使用します。特定のサーバグループを作成するには、**aaa group server radius** および **aaa group server tacacs+** コマンドを使用します。

Cisco IOS XE ソフトウェアは次の 2 つのアカウント方式をサポートします。

- **RADIUS:** ネットワーク アクセス サーバは、アカウントレコードの形式で RADIUS セキュリティサーバに対してユーザアクティビティを報告します。各アカウントレコードにはアカウントの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。

- **TACACS+**: ネットワークアクセスサーバは、アカウントングレコードの形式でTACACS+セキュリティサーバに対してユーザアクティビティを報告します。各アカウントングレコードにはアカウントングのAttribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。

アカウントングの方式リストは、アカウントングの実行方法を定義します。名前付きアカウントング方式リストにより、特定の回線またはインターフェイスで、特定の種類のアカウントングサービスに使用する特定のセキュリティプロトコルを指定できます。*list-name* および *method* を入力してリストを作成します。*list-name* にはこのリストの名前として使用する任意の文字列（*radius* や *tacacs+* などの方式名を除く）を指定し、*method* には指定されたシーケンスで試行する方式を指定します。

特定のアカウントングの種類の **aaa accounting** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線（このアカウントングの種類が適用される）にデフォルトの方式リストが自動的に適用されます（定義済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、アカウントングは実行されません。



Note システムアカウントングでは名前付きアカウントングリストは使用されず、システムアカウントングのためのデフォルトのリストだけを定義できます。

最小のアカウントングの場合、**stop-only** キーワードを指定して、要求されたユーザプロセスの終了時に **stop** レコードアカウントング通知を送信します。詳細なアカウントングの場合、**start-stop** キーワードを指定することで、**RADIUS** または **TACACS+** が要求されたプロセスの開始時に **start** アカウントング通知を送信し、プロセスの終了時に **stop** アカウントング通知を送信するようにできます。アカウントングは **RADIUS** または **TACACS+** サーバにだけ保存されます。**none** キーワードは、指定した回線またはインターフェイスのアカウントングサービスをディセーブルにします。

AAAアカウントングがアクティブにされると、ネットワークアクセスサーバは、ユーザが実装したセキュリティ方式に応じて、接続に関する **RADIUS** アカウントング属性または **TACACS+ AV** ペアをモニタします。ネットワークアクセスサーバはこれらの属性をアカウントングレコードとしてレポートし、アカウントングレコードはその後セキュリティサーバのアカウントングログに保存されます。



Note このコマンドは、**TACACS** または拡張 **TACACS** には使用できません。

次の例では、デフォルトのコマンドアカウントング方式リストを定義しています。この例のアカウントングサービスは **TACACS+** セキュリティサーバによって提供され、**stop-only** 制限で特権レベル 15 コマンドに設定されています。

```
Device> enable
Device# configure terminal
Device(config)# aaa accounting commands 15 default stop-only group TACACS+
Device(config)# exit
```

次の例では、アカウントサービスが TACACS+ セキュリティサーバで提供され、stop-only 制限があるデフォルトの auth-proxy アカウント方式リストの定義を示します。aaa accounting コマンドは認証プロキシアカウントをアクティブにします。

```
Device> enable
Device# configure terminal
Device(config)# aaa new model
Device(config)# aaa authentication login default group TACACS+
Device(config)# aaa authorization auth-proxy default group TACACS+
Device(config)# aaa accounting auth-proxy default start-stop group TACACS+
Device(config)# exit
```

aaa accounting dot1x

認証、認可、およびアカウントティング（AAA）アカウントティングをイネーブルにして、IEEE802.1X セッションの特定のアカウントティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1X アカウントティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+}... ]}
no aaa accounting dot1x {name | default}
```

Syntax Description

name	サーバグループ名。これは、 broadcast group および group キーワードの後に入力する場合に使用するオプションです。
default	デフォルトリストにあるアカウントティング方式を、アカウントティングサービス用に指定します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。 start アカウントティングレコードはバックグラウンドで送信されます。アカウントティングサーバが start accounting 通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウントティングレコードをイネーブルにして、アカウントティングレコードを各グループの最初のサーバに送信します。最初のサーバが使用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。
group	アカウントティングサービスに使用するサーバグループを指定します。有効なサーバグループ名は次のとおりです。 <ul style="list-style-type: none"> • name: サーバグループの名前。 • radius: すべての RADIUS ホストのリスト。 • tacacs+: すべての TACACS+ ホストのリスト。 broadcast group および group キーワードの後に入力する場合、 group キーワードはオプションです。オプションの group キーワードより多くの値を入力できます。
radius	(任意) RADIUS アカウントティングをイネーブルにします。
tacacs+	(任意) TACACS+ アカウントティングをイネーブルにします。

Command Default

AAA アカウントティングはディセーブルです。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、RADIUS サーバへのアクセスが必要です。
インターフェイスに IEEE 802.1X RADIUS アカウンティングを設定する前に、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

次の例では、IEEE 802.1X アカウンティングを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# exit
```

aaa accounting identity

IEEE 802.1X、MAC 認証バイパス（MAB）、および Web 認証セッションの認証、認可、およびアカウントリング（AAA）アカウントリングをイネーブルにするには、グローバル コンフィギュレーション モードで、**aaa accounting identity** コマンドを使用します。IEEE 802.1X アカウントリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
aaa accounting identity {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+}... ]}
no aaa accounting identity {name | default}
```

Syntax Description

name	サーバグループ名。これは、 broadcast group および group キーワードの後に入力する場合に使用するオプションです。
default	デフォルトリストにあるアカウントリング方式を、アカウントリングサービス用に使 用します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。 start アカウントリングレコードはバックグラウンドで送信されま す。アカウントリングサーバが start アカウントリング通知を受け取ったかどうかには 関係なく、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウントリングレコードをイネーブルにして、ア カウントリングレコードを各グループの最初のサーバに送信します。最初のサーバが 利用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバ を識別します。
group	アカウントリングサービスに使用するサーバグループを指定します。有効なサーバグ ループ名は次のとおりです。 <ul style="list-style-type: none"> • name: サーバグループの名前。 • radius: すべての RADIUS ホストのリスト。 • tacacs+: すべての TACACS+ ホストのリスト。 broadcast group および group キーワードの後に入力する場合、 group キーワードは オプションです。オプションの group キーワードより多くの値を入力できます。
radius	(任意) RADIUS 認証をイネーブルにします。
tacacs+	(任意) TACACS+ アカウントリングをイネーブルにします。

Command Default

AAA アカウントリングはディセーブルです。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

AAA アカウンティング アイデンティティをイネーブルにするには、ポリシー モードをイネーブルにする必要があります。ポリシーモードを有効にするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

次の例では、IEEE 802.1X アカウンティング アイデンティティを設定する方法を示します。

```
Device# authentication display new-style
```

Please note that while you can revert to legacy style configuration at any time unless you have explicitly entered new-style configuration, the following caveats should be carefully read and understood.

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
```

```
Device(config)# aaa accounting identity default start-stop group radius
```

```
Device(config)# exit
```

aaa authentication dot1x

IEEE 802.1X 認証に準拠するポートで使用する認証、許可、およびアカウントिंग（AAA）方式を指定するには、グローバルコンフィギュレーションモードで **aaa authentication dot1x** コマンドを使用します。認証を無効にするには、このコマンドの **no** 形式を使用します。

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

Syntax Description	<p>default ユーザがログインするときのデフォルトの方法。この引数に続いてリストされた認証方式が使用されます。</p> <p>method1 サーバ認証を指定します。認証用にすべての RADIUS サーバの一覧を使用するには、group radius キーワードを入力します。</p> <p>Note コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは default および group radius キーワードのみです。</p>				
Command Default	認証は実行されません。				
Command Modes	グローバル コンフィギュレーション (config)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	<p>method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために特定の順序で試みる方式を指定します。IEEE 802.1X に準拠している唯一の方式は、クライアントデータが RADIUS 認証サーバに対して確認される group radius 方式です。</p> <p>group radius を指定した場合、radius-server host グローバル コンフィギュレーション コマンドを入力して RADIUS サーバを設定する必要があります。</p> <p>設定された認証方式の一覧を表示するには、show running-config 特権 EXEC コマンドを使用します。</p> <p>次の例では AAA をイネーブルにして IEEE 802.1X 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。</p> <pre>Device> enable Device# configure terminal Device(config)# aaa new-model Device(config)# aaa authentication dot1x default group radius Device(config)# exit</pre>				

aaa new-model

認証、認可、およびアカウントिंग（AAA）アクセス制御モデルを有効にするには、グローバル コンフィギュレーション モードで **aaa new-model** コマンドを使用します。AAA アクセス制御モデルを無効にするには、このコマンドの **no** 形式を使用します。

```
aaa new-model
no aaa new-model
```

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default AAA が有効になっていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドにより、AAA アクセス制御システムが有効になります。

仮想端末回線（VTY）に関して **login local** コマンドが設定されている場合、**aaa new-model** コマンドを削除するときは、スイッチをリロードしてデフォルト設定または **login** コマンドを取得する必要があります。スイッチをリロードしない場合、スイッチは、VTYではデフォルトで **login local** コマンドに設定されます。



Note **aaa new-model** コマンドを削除することは推奨されません。

Examples

次に、AAA を初期化する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# exit
```

次に、VTY が設定済みで **aaa new-model** コマンドが削除された例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
```

```
login local !<=== Login local instead of "login"
line vty 5 15
login local
!
```

Related Commands

Command	Description
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。
aaa authentication arap	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
aaa authentication enable default	ユーザが特権コマンドレベルにアクセスできるかどうかを決定する AAA 認証を有効にします。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authentication ppp	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。

authentication host-mode

ポートで認証マネージャモードを設定するには、インターフェイスコンフィギュレーションモードで **authentication host-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication host-mode { **multi-auth** | **multi-domain** | **multi-host** | **single-host** }
no authentication host-mode

Syntax Description	multi-auth	multi-domain	multi-host	single-host
	ポートのマルチ認証モード (multi-auth モード) をイネーブルにします。	ポートのマルチドメインモードをイネーブルにします。	ポートのマルチホストモードをイネーブルにします。	ポートのシングルホストモードをイネーブルにします。

Command Default シングルホストモードがイネーブルにされています。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 接続されているデータ ホストが 1 つだけの場合は、シングルホストモードを設定する必要があります。シングルホストポートでの認証のために音声デバイスを接続しないでください。ポートで音声 VLAN が設定されていないと、音声デバイスの許可が失敗します。

データホストが IP フォン経由でポートに接続されている場合は、マルチドメインモードを設定する必要があります。音声デバイスを認証する必要がある場合は、マルチドメインモードを設定する必要があります。

ハブの背後にデバイスを配置し、それぞれを認証してポートアクセスのセキュリティを確保できるようにするには、マルチ認証モードに設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは 1 つだけです。

マルチホストモードでも、ハブ越しの複数ホストのためのポートアクセスが提供されますが、マルチホストモードでは、最初のユーザが認証された後でデバイスに対して無制限のポートアクセスが与えられます。

次の例では、ポートのマルチ認証モードをイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
```

```
Device(config-if)# authentication host-mode multi-auth
Device(config-if)# end
```

次の例では、ポートのマルチドメインモードをイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode multi-domain
Device(config-if)# end
```

次の例では、ポートのマルチホストモードをイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode multi-host
Device(config-if)# end
```

次の例では、ポートのシングルホストモードをイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode single-host
Device(config-if)# end
```

設定を確認するには、**show authentication sessions interface *interface* details** 特権 EXEC コマンドを入力します。

authentication logging verbose

認証システムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **authentication logging verbose** コマンドをグローバルコンフィギュレーションモードで使用します。

authentication logging verbose
no authentication logging verbose

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

システムメッセージの詳細ログは有効になっていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドにより、認証システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 認証システムメッセージをフィルタリングするには、次の手順に従います。

```
Device> enable
Device# configure terminal
Device(config)# authentication logging verbose
Device(config)# exit
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

Related Commands

コマンド	説明
authentication logging verbose	認証システムメッセージのフィルタリング
dot1x logging verbose	802.1X システムメッセージのフィルタリング
mab logging verbose	MAC 認証システムメッセージのフィルタリング

authentication mac-move permit

デバイス上での MAC 移動をイネーブルにするには、グローバル コンフィギュレーション モードで **authentication mac-move permit** コマンドを使用します。MAC 移動をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication mac-move permit
no authentication mac-move permit

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default MAC 移動は無効になっています。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドを使用すると、認証済みホストをデバイス上の認証対応ポート (MAC 認証バイパス (MAB)、802.1X、または Web-auth) 間で移動することができます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC 移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

次の例では、デバイス上で MAC 移動をイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# authentication mac-move permit
Device(config)# exit
```

Related Commands

コマンド	説明
access-session mac-move deny	デバイスで MAC 移動をディセーブルにします。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1X 認証をサポートしないクライアントを使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャモードを設定します。
authentication open	ポートでオープンアクセスをイネーブルまたはディセーブルにします。

コマンド	説明
authentication order	ポートで使用する認証方式の順序を設定し
authentication periodic	ポートの再認証をイネーブまたはディセ
authentication port-control	ポートの認証ステートの手動制御をイネー
authentication priority	ポートプライオリティリストに認証方式を
authentication timer	802.1X 対応ポートのタイムアウトパラメー
authentication violation	新しいデバイスがポートに接続するか、ポ るときに、新しいデバイスがポートに接続し
show authentication	デバイスの認証マネージャイベントに関する

authentication priority

プライオリティリストに認証方式を追加するには、インターフェイス コンフィギュレーション モードで **authentication priority** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

```
authentication priority [dot1x | mab] {webauth}
no authentication priority [dot1x | mab] {webauth}
```

Syntax Description	dot1x	(任意) 認証方式の順序に 802.1X を追加します。
	mab	(任意) 認証方式の順序に MAC 認証バイパス (MAB) を追加します。
	webauth	認証方式の順序に Web 認証を追加します。

Command Default デフォルトのプライオリティは、802.1X 認証、MAC 認証バイパス、Web 認証の順です。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 順序付けでは、デバイスがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。

ポートにフォールバック方式を複数設定するときは、Web 認証 (webauth) を最後に設定してください。

異なる認証方式にプライオリティを割り当てることにより、プライオリティの高い方式を、プライオリティの低い進行中の認証方式に割り込ませることができます。



Note クライアントがすでに認証されている場合に、プライオリティの高い方式の割り込みが発生すると、再認証されることがあります。

認証方式のデフォルトのプライオリティは、実行リストの順序におけるその位置と同じで、802.1X 認証、MAC 認証バイパス (MAB)、Web 認証の順です。このデフォルトの順序を変更するには、キーワード **dot1x**、**mab**、および **webauth** を使用します。

次の例では、802.1X を最初の認証方式、Web 認証を 2 番目の認証方式として設定する方法を示します。

```
Device(config-if)# authentication priority dot1x webauth
```

次の例では、MAB を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# authentication priority mab webauth
Device(config-if)# end
```

Related Commands

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event fail	認証マネージャが認証エラーを認識されないユーザクレデンシャルを拒否して、セッションを再初期化します。
authentication event no-response action	認証マネージャが認証エラーを応答のないホストの結果として拒否して、セッションを再初期化します。
authentication event server alive action reinitialize	以前に到達不能であった認証、許可、アカウントिंगサーバが再び到達可能になると、認証マネージャセッションを再初期化します。
authentication event server dead action authorize	認証、許可、アカウントिंगサーバが到達不能になったときに、セッションを再初期化します。
authentication fallback	Web 認証のフォールバック方式をイネーブルにします。
authentication host-mode	ホストの制御ポートへのアクセスを許可します。
authentication open	ポートでオープンアクセスをイネーブルにします。
authentication order	認証マネージャがポート上のクライアントの認証を試みる順序を指定します。
authentication periodic	ポートの自動再認証をイネーブルにします。
authentication port-control	制御ポートの許可ステータスを設定します。
authentication timer inactivity	機能しない認証マネージャセッションを強制終了するまでの時間を指定します。
authentication timer reauthenticate	認証マネージャが許可ポートの再認証を試みる間隔を指定します。
authentication timer restart	認証マネージャが無許可ポートの認証を試みる間隔を指定します。
authentication violation	ポート上でセキュリティ違反が生じた場合に取りうるアクションを指定します。
mab	ポートの MAC 認証バイパスをイネーブルにします。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャセッションに関する情報を表示します。

コマンド	説明
show authentication sessions interface	特定のインターフェイスの認証マネージャに関する情報を表示

authentication violation

新しいデバイスがポートに接続されたとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続されたときに発生する違反モードを設定するには、インターフェイス コンフィギュレーション モードで **authentication violation** コマンドを使用します。

```
authentication violation { protect | replace | restrict | shutdown }
no authentication violation { protect | replace | restrict | shutdown }
```

Syntax Description	protect	replace	restrict	shutdown
	予期しない着信 MAC アドレスをドロップします。syslog エラーは生成されません。	現在のセッションを削除し、新しいホストによる認証を開始します。	違反エラーの発生時に Syslog エラーを生成します。	エラーによって、予期しない MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。

Command Default Authentication violation shutdown モードがイネーブルにされています。

Command Modes インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ポート上でセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

次の例では、新しいデバイスがポートに接続する場合に、errdisable になり、シャットダウンするように IEEE 802.1X 対応ポートを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation shutdown
Device(config-if)# end
```

次の例では、新しいデバイスがポートに接続する場合に、システムエラーメッセージを生成して、ポートを制限モードに変更するように 802.1X 対応ポートを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
```

```
Device(config-if)# authentication violation restrict
Device(config-if)# end
```

次の例では、新しいデバイスがポートに接続するときに、そのデバイスを無視するように 802.1X 対応ポートを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation protect
Device(config-if)# end
```

次の例では、新しいデバイスがポートに接続するときに、現在のセッションを削除し、新しいデバイスによる認証を開始するように 802.1X 対応ポートを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation replace
Device(config-if)# end
```

設定を確認するには、**show running-config interface interface-name** コマンドを入力します。

cisp enable

デバイス上で Client Information Signalling Protocol (CISP) をイネーブルにして、サブリカントデバイスのオーセンティケータとして機能し、オーセンティケータデバイスのサブリカントとして機能するようにするには、**cisp enable** グローバル コンフィギュレーション コマンドを使用します。

cisp enable
no cisp enable

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

デフォルトの動作や値はありません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

オーセンティケータとサブリカントデバイス間のリンクはトランクです。両方のデバイスで VTP をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードがサーバである必要があります。

VTP モードを設定する場合に MD5 チェックサムの一一致エラーにならないようにするために、次の点を確認してください。

- VLAN が異なる 2 台のデバイスに設定されていないこと。同じドメインに VTP サーバが 2 台存在することがこの状態の原因になることがあります。
- 両方のデバイスで、設定のリビジョン番号が異なっていること。

次の例では、CISP をイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# cisp enable
Device(config)# exit
```

Related Commands

コマンド	説明
dot1x credentials プロファイル	プロファイルをサブリカントデバイスに設定
dot1x supplicant force-multicast	802.1X サブリカントがマルチキャストパケットに強制します。
dot1x supplicant controlled transient	802.1X サブリカントによる制御アクセスを

コマンド	説明
show cisp	指定されたインターフェイスの CISP 情報を表示

clear errdisable interface vlan

error-disabled 状態になっていた VLAN を再びイネーブルにするには、特権 EXEC モードで **clear errdisable interface** コマンドを使用します。

```
clear errdisable interface interface-id vlan [vlan-list]
```

Syntax Description	interface-id	インターフェイスを指定します。
	vlan list	(任意) 再びイネーブルにする VLAN のリストを の VLAN が再びイネーブルになります。

Command Default デフォルトの動作や値はありません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **shutdown** および **no shutdown** のインターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにするか、**clear errdisable** インターフェイスコマンドを使用して VLAN の error-disabled をクリアできます。

Examples

次の例では、ギガビットイーサネットポート 4/0/2 で errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

Related Commands	コマンド	説明
	errdisable detect cause	特定の原因、またはすべての原因をリストアップします。
	errdisable recovery	回復メカニズム変数を設定します。
	show errdisable detect	errdisable 検出ステータスを表示します。
	show errdisable recovery	errdisable 回復タイマーの情報を表示します。
	show interfaces status err-disabled	errdisable ステートになっているインターフェイスのステータスを表示します。

clear mac address-table

特定のダイナミックアドレス、特定のインターフェイス上のすべてのダイナミックアドレス、スタックメンバ上のすべてのダイナミックアドレス、または特定の VLAN 上のすべてのダイナミックアドレスを MAC アドレステーブルから削除するには、**clear mac address-table** コマンドを特権 EXEC モードで使用します。このコマンドはまた MAC アドレス通知グローバルカウンタもクリアします。

```
clear mac address-table {dynamic [address mac-addr | interface interface-id | vlan vlan-id]
| move update | notification}
```

Syntax Description		
dynamic		すべてのダイナミック MAC アドレスを削除します。
address mac-addr		(任意) 指定されたダイナミック MAC アドレスを削除します。
interface interface-id		(任意) 指定された物理ポートまたはポートチャネル上のすべてのダイナミックアドレスを削除します。
vlan vlan-id		(任意) 指定された VLAN のすべてのダイナミックアドレスを削除します。
move update		MAC アドレステーブルの move-update カウンタをリセットします。
notification		履歴テーブルの通知をクリアし、カウンタをリセットします。

Command Default デフォルトの動作や値はありません。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 情報が削除されたことを確認するには、**show mac address-table** コマンドを入力します。

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
Device> enable
Device# clear mac address-table dynamic address 0008.0070.0007
```

Related Commands	コマンド	説明
	mac address-table notification	MAC アドレス通知機能をイネーブルにします。

コマンド	説明
mac address-table move update {receive transmit}	デバイスの MAC アドレステーブル移動更新を設定します。
show mac address-table	MAC アドレステーブルのスタティックエントリおよびダイナミックエントリを表示します。
show mac address-table move update	デバイスに関する MAC アドレステーブル移動更新情報を表示します。
show mac address-table notification	interface キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC アドレス通知トラップをイネーブルにします。

confidentiality-offset

MACsec Key Agreement (MKA) プロトコルを有効にして MACsec 動作の機密性オフセットを設定するには、MKA ポリシー コンフィギュレーション モードで **confidentiality-offset** コマンドを使用します。機密性オフセットを無効にするには、このコマンドの **no** 形式を使用します。

confidentiality-offset
no confidentiality-offset

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default 機密性オフセットが無効になっています。

Command Modes MKA ポリシー コンフィギュレーション (config-mka-policy)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、機密性オフセットを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# confidentiality-offset
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

crypto pki trustpool import

既存の認証局（CA）証明書バンドルを更新または交換するために CA 証明書バンドルを公開キーインフラストラクチャ（PKI）トラストプールにインポート（ダウンロード）するには、グローバル コンフィギュレーション モードで **crypto pki trustpool import** コマンドを使用します。設定されたパラメータをすべて削除するには、このコマンドの **no** 形式を使用します。

crypto pki trustpool import {ca-bundle | clean [terminal | url url] | terminal | url url}

no crypto pki trustpool import {ca-bundle | clean [terminal | url url] | terminal | url url}

Syntax Description

ca-bundle	トラストプールポリシーで設定されている CA 証明書バンドルをインポートします。
clean	新しい証明書をダウンロードする前に、ダウンロード済みの PKI トラストプール証明書を削除します。既存の CA 証明書バンドルの端末設定を削除する場合はオプションの terminal キーワードを使用し、URL ファイルシステム設定を削除する場合は url キーワードと <i>url</i> 引数を使用します。
terminal	CA 証明書バンドルをプライバシー強化メール（PEM）の形式で端末からカットアンドペーストでインポートします。
url url	指定した URL から CA 証明書バンドルをインポートします。

Command Default

PKI トラストプール機能が有効になっています。PKI トラストプール内の組み込みの CA 証明書バンドルがデバイスで使用されます。このバンドルは自動的に更新されます。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines

PKI トラストプール証明書は自動的に更新されます。PKI トラストプール証明書が最新でない場合は、**crypto pki trustpool import** コマンドを使用して別の場所から更新します。



Note セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶えず変化しています。最新のシスコの暗号化に関する推奨事項については、『[Next Generation Cryptography](#)』ホワイトペーパーを参照してください。

url 引数で CA の URL ファイルシステムを指定または変更します。次の表に、使用可能な URL ファイルシステムを示します。

Table 142: URL ファイルシステム

ファイルシステム	説明
archive:	アーカイブファイルシステムからインポートします。
cns:	クラスタ名前空間（CNS）ファイルシステムからインポートします。
disk0:	disk0 ファイルシステムからインポートします。
disk1:	disk1 ファイルシステムからインポートします。
ftp:	FTP ファイルシステムからインポートします。
http:	<p>HTTP ファイルシステムからインポートします。URL は次の形式にする必要があります。</p> <ul style="list-style-type: none"> • <code>http://CName:80</code>: <i>CName</i> はドメインネームシステム（DNS）です。 • <code>http://ipv4-address:80</code>: たとえば、<code>http://10.10.10.1:80</code> のようになります。 • <code>http://[ipv6-address]:80</code>: たとえば、<code>http://[2001:DB8:1:1::1]:80</code> のようになります。URL 内の IPv6 アドレスは 16 進数表記とし、括弧で囲む必要があります。
https:	HTTPS ファイルシステムからインポートします。URL は HTTP: ファイルシステムの形式と同じ形式にする必要があります。
null:	null ファイルシステムからインポートします。
nvrn:	NVRAM ファイルシステムからインポートします。
pram:	パラメータ ランダムアクセス メモリ（PRAM）ファイルシステムからインポートします。
rep:	リモートコピープロトコル（RCP）ファイルシステムからインポートします。
scp:	Secure Copy Protocol（SCP）ファイルシステムからインポートします。
snmp:	Simple Network Management Protocol（SNMP）ファイルシステムからインポートします。
system:	システムファイルからインポートします。
tar:	UNIX TAR ファイルシステムからインポートします。
tftp:	<p>TFTP ファイルシステムからインポートします。</p> <p>Note URL は <code>tftp://CName/filespecification</code> の形式にする必要があります。</p>
tmpsys:	Cisco IOS tmpsys ファイルシステムからインポートします。

ファイルシステム	説明
unix:	UNIX ファイルシステムからインポートします。
xmodem:	xmodem 簡易ファイル転送プロトコルシステムからインポートします。
ymodem:	ymodem 簡易ファイル転送プロトコルシステムからインポートします。

Examples

次に、ダウンロード済みのすべてのPKIトラストプールCA証明書を削除してから、新しいCA証明書バンドルをダウンロードしてPKIトラストプール内のCA証明書を更新する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto pki trustpool import clean
```

次に、ダウンロード済みのPKIトラストプールCA証明書は削除せずに、新しいCA証明書バンドルをダウンロードしてPKIトラストプール内のすべてのCA証明書を更新する例を示します。

```
Device (config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

Related Commands

コマンド	説明
crypto pki trustpool policy	PKIトラストプールポリシーパラメータを設定します。
show crypto pki trustpool	デバイスのPKIトラストプール証明書を表示し、オプションでPKIトラストプールポリシーを表示します。

debug aaa dead-criteria transaction

認証、許可、およびアカウントिंग（AAA）の dead-criteria ランザクション値を表示するには、**debugaaadead-criteriatransaction** コマンドを特権 EXEC モードで使用します。dead-criteria のデバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug aaa dead-criteria transaction
no debug aaa dead-criteria transaction

Syntax Description	このコマンドには引数またはキーワードはありません。
Command Default	コマンドが設定されていない場合、デバッグはオンになりません。
Command Modes	特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines dead-criteria トランザクションの値は、AAA トランザクションごとに異なる場合があります。表示される可能性のある値の一部は、推定される未処理の トランザクション、再送信の試行、および dead 検出間隔です。これらの値については、次の表で説明します。

Examples

次に、特定のサーバグループの dead-criteria トランザクションの情報の例を示します。

```
Device> enable
Device# debug aaa dead-criteria transaction

AAA Transaction debugs debugging is on
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 10, Current Tries: 3,
Current Max Tries: 10
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 10s, Elapsed Time:
317s, Current Max Interval: 10s
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transaction: 6, Current Max
Transaction: 6
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 143: debug aaa dead-criteria transaction フィールドの説明

フィールド	説明
AAA/SG/TRANSAC	AAA サーバグループ トランザクション。
Computed Retransmit Tries	サーバが dead としてマークされるまでの、現在計算されている再送信回数。
Current Tries	最後の有効な応答以降の連続失敗回数。

フィールド	説明
Current Max Tries	最後に成功したトランザクション以降の最大試行回数。
Computed Dead Detect Interval	サーバが dead としてマークされる前に経過する可能性がある非アクティブ期間（最後の正常なトランザクションからの秒数）。非アクティブ期間は、 live と見なされるサーバにランザクションが送信されたときに開始されます。 dead 検出間隔は、デバイスがサーバを dead としてマークする前に、サーバからの応答をデバイスが待機する期間です。
経過時間（Elapsed Time）	最後の有効な応答以降に経過した時間。
Current Max Interval	最後に成功したトランザクション以降の非アクティブ期間の最大値。
Estimated Outstanding Transaction	サーバに関連付けられているトランザクションの推定数。
Current Max Transaction	最後に成功したトランザクション以降の最大トランザクション。

Related Commands

コマンド	説明
radius-server dead-criteria	RADIUS サーバをデッド状態と指定するための条件のいずれかまたは両方を、指定した定数で適用します。
show aaa dead-criteria	AAA サーバの dead-criteria 検出情報を表示します。

debug umbrella

Cisco Umbrella 統合機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug umbrella** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug umbrella {config | device-registration | dnscrypt | redundancy}
no debug umbrella {config | device-registration | dnscrypt | redundancy}
```

Syntax Description

config	設定のデバッグをイネーブルにします。
device-registration	デバイス登録のデバッグをイネーブルにします。
dnscrypt	DNSCrypt のデバッグをイネーブルにします。
redundancy	冗長性のデバッグをイネーブルにします。

Command Default

デバッグはディセーブルです。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、Cisco Umbrella の設定のデバッグをイネーブルにする例を示します。

```
Device> enable
Device# debug umbrella config

Umbrella config debugging is on

Device# configure terminal
Device(config)# interface gigabitethernet 1/0/12
Device(config-if)# umbrella in test

*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Umbrella token configured, so set mode as TOKEN
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:check user configured resolver count
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Umbrella interface with no direct cloud access
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Umbrella mandatory parameter 'token' or
'api-key/secret/orgid' configured
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Processing is umbrella enabled check
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Is umbrella enabled check failed:sw idb info not found
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Send the interface info to device registration proces
*Nov 27 08:34:41.089: UMBRELLA-CONFIG:Add interface GigabitEthernet1/0/12 request sent to
DP
*Nov 27 08:34:41.089: UMBRELLA-CONFIG:Configured 'umbrella in test' on interface
GigabitEthernet1/0/12
*Nov 27 08:34:41.089: UMBRELLA-CONFIG:Cannot add domain patterns to DSA: Nothing to add
```

delay-protection

MACsec Key Agreement Protocol Data Unit (MKPDU) の送信に遅延保護を使用するように MKA を設定するには、MKA ポリシー コンフィギュレーションモードで **delay-protection** コマンドを使用します。遅延保護を無効にするには、このコマンドの **no** 形式を使用します。

delay-protection
no delay-protection

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

MKPDU の送信に対する遅延保護は無効になっています。

Command Modes

MKA ポリシー コンフィギュレーション (config-mka-policy)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、MKPDU の送信で遅延保護を使用するように MKA を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# delay-protection
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

deny (MAC アクセス リスト コンフィギュレーション)

条件が一致した場合に非 IP トラフィックが転送されないようにするには、MAC アクセスリスト拡張コンフィギュレーションモードで **deny** コマンドを使用します。名前付き MAC アクセスリストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

```
deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-udp] [cos cos]
no deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-udp] [cos cos]
```

Syntax Description

any	すべての送信元または宛先 MAC アドレスを拒否します。
host src-MAC-addr src-MAC-addr mask	ホスト MAC アドレスと任意のサブネットマスクが定義されたアドレスに一致するトラフィックは拒否されます。
host dst-MAC-addr dst-MAC-addr mask	宛先 MAC アドレスと任意のサブネットマスクが定義されたアドレスに一致する場合、トラフィックは拒否されます。
type mask	(任意) パケットの EtherType 番号と、EtherType とマスクを使用して、パケットのプロトコルを識別します。 type には、0 ~ 65535 の 16 進数を指定できます。 mask は、一致をテストする前に EtherType に一致する必要があります。
aarp	(任意) データリンクアドレスをネットワーク上で解決する AppleTalk Address Resolution Protocol を指定します。
amber	(任意) EtherType DEC-Amber を指定します。
appletalk	(任意) EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	(任意) EtherType Digital Equipment Corporation Spanning Tree Protocol を指定します。
decnet-iv	(任意) EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	(任意) EtherType DEC-Diagnostic を指定します。
dsm	(任意) EtherType DEC-DSM を指定します。

etype-6000	(任意) EtherType 0x6000 を指定します。
etype-8042	(任意) EtherType 0x8042 を指定します。
lat	(任意) EtherType DEC-LAT を指定します。
lavc-sca	(任意) EtherType DEC-LAVC-SCA を指定します。
lsap <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と、パケットの プロトコルを指定します。 <i>mask</i> は、一致をテストする前に LSAP 番号を マスクする必要があります。
mop-console	(任意) EtherType DEC-MOP Remote Console を指定します。
mop-dump	(任意) EtherType DEC-MOP Dump を指定します。
msdos	(任意) EtherType DEC-MSDOS を指定します。
mumps	(任意) EtherType DEC-MUMPS を指定します。
netbios	(任意) EtherType DEC-Network Basic Input/Output Protocol を指定します。
vines-echo	(任意) Banyan Systems による EtherType DEC-VINES Echo を指定します。
vines-ip	(任意) EtherType VINES IP を指定します。
xns-idp	(任意) 10 進数、16 進数、または 8 進数の XNS IDP Network Systems (XNS) プロトコルスイートを指定します。
cos <i>cos</i>	(任意) プライオリティを設定するために、CoS を指定します。 CoS に基づくフィルタリングを行います。 cos オプションが設定されているかどうかを確認 できます。

Command Default

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

Command Modes

MAC アクセスリスト拡張コンフィギュレーション (config-ext-macl)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

MAC アクセスリスト拡張コンフィギュレーションモードを開始するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

host キーワードを使用した場合、アドレスマスクは入力できません。**host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセスコントロールエントリ (ACE) がアクセスコントロールリストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap lsap mask** キーワードを使用します。Novell 用語と Cisco IOS XE 用語での IPX カプセル化タイプに対応するフィルタ条件を表に一覧表示します。

Table 144: IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS XE 名	Novel 名	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセスリストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
Device(config-ext-macl)# end
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
Device(config-ext-macl)# end
```

次に、EtherType 0x4321 のすべてのパケットを拒否する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any any 0x4321 0
Device(config-ext-macl)# end
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

Related Commands

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベー
permit	MAC アクセスリスト コンフィギュレーシ 条件が一致した場合に非 IP トラフィックが
show access-lists	デバイスに設定されたアクセス制御リスト

device-role (IPv6 スヌーピング)

ポートに接続されているデバイスのロールを指定するには、IPv6 スヌーピング コンフィギュレーションモードで **device-role** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

```
device-role {node | switch}
no device-role {node | switch}
```

Syntax Description

node 接続されたデバイスのロールをノードに設定します。

switch 接続されたデバイスのロールをデバイスに設定します。

Command Default

デバイスのロールはノードです。

Command Modes

IPv6 スヌーピング コンフィギュレーション (config-ipv6-snooping)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはノードです。

switch キーワードは、リモートデバイスがスイッチであり、ローカルスイッチがマルチスイッチモードで動作していることを示します。ポートで学習したバインディングエントリは、**trunk_port** プリファレンス レベルでマークされます。ポートが **trusted** ポートに設定されている場合、バインディングエントリは **trunk_trusted_port** プリファレンス レベルでマークされます。

次に、IPv6 スヌーピング ポリシー名を **policy1** と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、デバイスをノードとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
Device(config-ipv6-snooping)# end
```

device-role (IPv6 ND インスペクション)

ポートに接続されているデバイスのロールを指定するには、ネイバー探索 (ND) インスペクション ポリシー コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {host | switch}

Syntax Description	host	接続されたデバイスのロールをホストに設定します。
	switch	接続されたデバイスのロールをスイッチに設定します。
Command Default	デバイスのロールはホストです。	
Command Modes	ND インスペクション ポリシー コンフィギュレーション (config-nd-inspection)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **device-role** コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはホストであるため、すべての着信ルータ アドバタイズメントとリダイレクトメッセージはブロックされます。

switch キーワードは、リモートデバイスがスイッチであり、ローカルスイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインディング エントリは、trunk_port プリファレンス レベルでマークされます。ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。

次に、Neighbor Discovery Protocol (NDP) ポリシー名を policy1 と定義し、デバイスを ND インスペクション ポリシー コンフィギュレーション モードにして、デバイスをホストとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
Device(config-nd-inspection)# end
```

device-tracking (インターフェイス コンフィギュレーション)

SISF ベースのデバイストラッキングをイネーブルにしてデフォルトポリシーをインターフェイスまたは VLAN にアタッチするか、その機能をイネーブルにしてカスタムポリシーをアタッチするには、インターフェイス コンフィギュレーション モードで **device-tracking** コマンドを入力します。ポリシーをインターフェイスまたは VLAN からデタッチしてデフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
device-tracking [ attach-policy policy-name ] [ vlan { vlan-id | add vlan-id | all | except vlan-id | none | remove vlan-id } ]
no device-tracking [ attach-policy policy-name ] [ vlan { vlan-id | add vlan-id | all | except vlan-id | none | remove vlan-id } ]
```

Syntax Description

attach-policy <i>policy-name</i>	指定したカスタムポリシーをインターフェイスおよびすべての VLAN にアタッチします。
vlan { <i>vlan-id</i> add <i>vlan-id</i> all except <i>vlan-id</i> none remove <i>vlan-id</i> }	<p>ポリシーの VLAN リストを設定し、指定された VLAN にカスタムポリシーをアタッチします。次の項目を指定できます。</p> <ul style="list-style-type: none"> • vlan-id: 1つ以上の VLAN ID を入力します。カスタムポリシーは、すべての VLAN ID にアタッチされます。 • addvlan-id: 指定された VLAN を既存の VLAN ID リストに追加します。カスタムポリシーは、すべての VLAN ID にアタッチされます。 • all: カスタムポリシーをすべての VLAN ID にアタッチします。これがデフォルトのオプションです。 • exceptvlan-id: ここで指定したものを除くすべての VLAN ID にカスタムポリシーをアタッチします。 • none: どの VLAN にもカスタムポリシーをアタッチしません。 <p>removevlan-id: 指定された VLAN を既存の VLAN ID リストから削除します。カスタムポリシーは、リスト内の VLAN ID にのみアタッチされます。</p>

Command Default

SISF ベースのデバイストラッキングはディセーブルになっており、ポリシーはインターフェイスにアタッチされません。

Command Modes

インターフェイス コンフィギュレーション (Device((config-if)#))

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

インターフェイス コンフィギュレーション モードで、他のキーワードを指定せずに **device-tracking** コマンドを入力すると、システムはデフォルトポリシーをインターフェイスまたは VLAN にアタッチします。デフォルトポリシーは、デフォルト設定の組み込みポリシーで、デフォルトポリシーの属性は変更できません。

インターフェイス コンフィギュレーション モードで **device-tracking attach-policy** *policy-name* コマンドを設定すると、カスタムポリシー名を指定できます。グローバル コンフィギュレーション モードでカスタムポリシーをすでに作成している必要があります。ポリシーは、指定されたインターフェイスにアタッチされます。その後、アタッチする VLAN を指定することもできます。

ターゲットにアタッチされるカスタムポリシーを変更する場合は、**device-tracking attach-policy** *policy-name* コマンドを再設定します。

特定のターゲットで機能をディセーブルにするには、インターフェイス コンフィギュレーション モードで **no device-tracking** コマンドを使用します。

例

- 例: SISF ベースのデバイストラッキングをイネーブルにして、デフォルトポリシーをアタッチする, [on page 1411](#)
- カスタムポリシーのアタッチ, [on page 1412](#)
- 例: SISF ベースのデバイストラッキングをディセーブルにする, [on page 1412](#)

Examples

次に、SISF ベースのデバイストラッキングをイネーブルにして、デフォルトポリシーをインターフェイスにアタッチする例を示します。デフォルトポリシーにはデフォルトポリシー パラメータがあり、変更することはできません。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# device-tracking
Device(config-if)# end

Device# show device-tracking policies detail
Target          Type Policy          Feature          Target range
Tel1/0/1        PORT default        Device-tracking vlan all
Tel1/0/2        PORT default        Device-tracking vlan all

Device-tracking policy default configuration:
 security-level guard
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP6
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
Policy default is applied on the following targets:
```

Target	Type	Policy	Feature	Target range
Te1/0/1	PORT	default	Device-tracking	vlan all
Te1/0/2	PORT	default	Device-tracking	vlan all

Examples

次に、SISF ベースのデバイストラッキングをイネーブルにして、sisf-01 というカスタムポリシーを上記の例と同じインターフェイス (Te1/0/1) にアタッチする例を示します。これにより、Te1/0/1 の既存のデフォルトポリシーがカスタムポリシー sif-01 に置き換えられます。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# device-tracking attach-policy sif-01
Device(config-if)# end

Device# show device-tracking policies detail
Target                Type Policy                Feature                Target range
Te1/0/1                PORT sif-01                Device-tracking       vlan all
Te1/0/2                PORT default              Device-tracking       vlan all

Device-tracking policy default configuration:
 security-level guard
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP6
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
Policy default is applied on the following targets:
Target                Type Policy                Feature                Target range
Te1/0/2                PORT default              Device-tracking       vlan all
Device-tracking policy sif-01 configuration:
 security-level guard
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP6
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
 limit address-count 3000
Policy sif-01 is applied on the following targets:
Target                Type Policy                Feature                Target range
Te1/0/1                PORT sif-01                Device-tracking       vlan all
```

Examples

次に、ターゲットで SISF ベースのデバイストラッキングをディセーブルにする例を示します。この機能はターゲット Te1/0/1 でディセーブルになります。これは、前の例でカスタムポリシーが適用されたものと同じインターフェイスです。デフォルトポリシーは、機能がイネーブルになっている他のインターフェイス (Te1/0/2) で引き続き使用できます。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# no device-tracking attach-policy sif-01
Device(config-if)# end

Device# show device-tracking policies detail
Target                Type Policy                Feature                Target range
Te1/0/2                PORT default              Device-tracking       vlan all
```

Device-tracking policy default configuration:

```
security-level guard
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP6
gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
```

Policy default is applied on the following targets:

Target	Type	Policy	Feature	Target range
Tel/0/2	PORT	default	Device-tracking	vlan all

device-tracking (VLAN コンフィギュレーション)

スイッチ統合型セキュリティ機能 (SISF) ベースのデバイストラッキングをイネーブルにしてデフォルトポリシーを VLAN にアタッチするか、その機能をイネーブルにしてカスタムポリシーを VLAN にアタッチし、ポリシーの優先順位を指定するには、VLAN コンフィギュレーションモードで **device-tracking** コマンドを入力します。ポリシーを VLAN からデタッチしてデフォルトに戻すには、このコマンドの **no** 形式を使用します。

device-tracking [*attach-policy policy-name*] [*priority priority-value*]

Syntax Description

attach-policy policy-name 指定されたカスタムポリシーを VLAN にアタッチします。

priority priority-value **Note** このコマンドは、CLI のヘルプに表示されますが、設定しても効果はありません。ポリシーの優先順位はシステムによって決定されます。これは変更できません。

Command Default

SISF ベースのデバイストラッキングはディセーブルになっています。

Command Modes

VLAN コンフィギュレーションモード (Device((config-vlan-config)#))

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Usage Guidelines

VLAN コンフィギュレーションモードで、他のキーワードを指定せずに **device-tracking** コマンドを入力すると、システムはデフォルトポリシーを VLAN にアタッチします。デフォルトポリシーは、デフォルト設定の組み込みポリシーであるため、デフォルトポリシーのパラメータは変更できません。

VLAN コンフィギュレーションモードで **device-tracking attach-policy policy-name** コマンドを設定すると、指定されたカスタムポリシーが VLAN にアタッチされます。カスタムポリシーを使用すると、カスタムポリシーの特定のパラメータを設定できます。

この機能をイネーブルにして、ポリシー (カスタムまたはデフォルト) を 1 つ以上の VLAN または VLAN 範囲にアタッチできます。

例

- 例: SISF ベースのデバイストラッキングをイネーブルにして、デフォルトポリシーをアタッチする, [on page 1415](#)
- 例: カスタムポリシーを VLAN にアタッチする, [on page 1415](#)
- 例: カスタムポリシーを VLAN 範囲にアタッチする, [on page 1415](#)

Examples

次に、SISF ベースのデバイストラッキングをイネーブルにして、デフォルトポリシーを VLAN 500 にアタッチする例を示します。

```
Device# show device-tracking policies
Target          Type Policy          Feature          Target range
Tel/0/1         PORT sisf-03       Device-tracking  vlan all
Tel/0/1         PORT default     Address Resolution Relay  vlan all
Tel/0/2         PORT default     Device-tracking  vlan all
vlan 333        VLAN sisf-01       Device-tracking  vlan all
```

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#vlan configuration 500
Device(config-vlan-config)# device-tracking
Device(config-vlan-config)# end
```

```
Device#show device-tracking policies
Target          Type Policy          Feature          Target range
Tel/0/1         PORT sisf-03       Device-tracking  vlan all
Tel/0/1         PORT default     Address Resolution Relay  vlan all
Tel/0/2         PORT default     Device-tracking  vlan all
vlan 333        VLAN sisf-01       Device-tracking  vlan allvlan 500
VLAN default          Device-tracking vlan all
```

Examples

次に、sisf-03 というカスタムポリシーを上記の例と同じ VLAN (VLAN 500) にアタッチする例を示します。これにより、VLAN 上の既存のデフォルトポリシーがカスタムポリシー sisf-03 に置き換えられます。

```
Device# show device-tracking policies
Target          Type Policy          Feature          Target range
Tel/0/1         PORT sisf-03       Device-tracking  vlan all
Tel/0/1         PORT default     Address Resolution Relay  vlan all
Tel/0/2         PORT default     Device-tracking  vlan all
vlan 333        VLAN sisf-01       Device-tracking  vlan all
vlan 500        VLAN default     Device-tracking  vlan all
```

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration 500
Device(config-vlan-config)# device-tracking attach-policy sisf-03
Device(config-vlan-config)# end
```

```
Device# show device-tracking policies
Target          Type Policy          Feature          Target range
Tel/0/1         PORT sisf-03       Device-tracking  vlan all
Tel/0/1         PORT default     Address Resolution Relay  vlan all
Tel/0/2         PORT default     Device-tracking  vlan all
vlan 333        VLAN sisf-01       Device-tracking  vlan allvlan 500
VLAN sisf-03          Device-tracking vlan all
```

Examples

次に、カスタムポリシーを VLAN 範囲 (VLAN 10 ~ 15) にアタッチする例を示します。

```
Device(config)# vlan configuration 10-15
Device(config-vlan-config)#device-tracking attach-policy sisf-01
Device(config-vlan-config)#end
```

```
Device# show device-tracking policies
```

Target	Type	Policy	Feature	Target range
Te1/0/2	PORT	default	Device-tracking	vlan all
vlan 10	VLAN	sisf-01	Device-tracking	vlan all
vlan 11	VLAN	sisf-01	Device-tracking	vlan all
vlan 12	VLAN	sisf-01	Device-tracking	vlan all
vlan 13	VLAN	sisf-01	Device-tracking	vlan all
vlan 14	VLAN	sisf-01	Device-tracking	vlan all
vlan 15	VLAN	sisf-01	Device-tracking	vlan all

device-tracking binding

バインディングテーブルでバインディングエントリを維持する方法を指定するには、グローバルコンフィギュレーションモードで **device-tracking binding** コマンドを入力します。このコマンドを使用すると、各状態のライフタイム、バインディングテーブルで許可されるエントリの最大数、およびバインディングエントリイベントをログに記録するかどうかを設定できます。このコマンドを使用して、スタティックバインディングエントリを設定することもできます。デフォルト値に戻すには、コマンドの **no** 形式を使用します。

device-tracking binding { **down-lifetime** | **logging** | **max-entries** | **reachable-lifetime** | **stale-lifetime** | **vlan** }

わかりやすくするために、上記の各オプションについて、その後続く残りのコマンド文字列を個別に示します。

- **device-tracking binding down-lifetime** { *seconds* | **infinite** }

no device-tracking binding down-lifetime

- **device-tracking binding logging**

no device-tracking binding logging

- **device-tracking binding max-entries** *no_of_entries* [**mac-limit** *no_of_entries* | **port-limit** *no_of_entries* [**mac-limit** *no_of_entries*] | **vlan-limit** *no_of_entries* [**mac-limit** *no_of_entries* | **port-limit** *no_of_entries* [**mac-limit** *no_of_entries*]]]

no device-tracking binding max-entries

- **device-tracking binding reachable-lifetime** { *seconds* | **infinite** } [**down-lifetime** { *seconds* | **infinite** } | **stale-lifetime** { *seconds* | **infinite** } [**down-lifetime** { *seconds* | **infinite** }]]

no device-tracking binding reachable-lifetime

- **device-tracking binding stale-lifetime** { *seconds* | **infinite** } [**down-lifetime** { *seconds* | **infinite** }]

no device-tracking binding stale-lifetime

- **device-tracking binding vlan** *vlan_id* { *ipv4_add* *ipv6_add* *ipv6_prefix* } [**interface** *interface_type_no*] [*48-bit-hardware-address*] [**reachable-lifetime** { *seconds* | **default** | **infinite** } **tracking** { **default** | **disable** | **enable** } **reachable-lifetime** { *seconds* | **default** | **infinite** }]

no device-tracking binding vlan *vlan_id* { *ipv4_add* *ipv6_add* *ipv6_prefix* } [**interface** *interface_type_no*] [*48-bit-hardware-address*] [**reachable-lifetime** { *seconds* | **default** | **infinite** } **tracking** { **default** | **disable** | **enable** } **reachable-lifetime** { *seconds* | **default** | **infinite** }]

Syntax Description

down-lifetime {
seconds | **infinite** }

DOWN 状態のバインディングエントリのカウンタダウンタイマーを設定するか、タイマーをディセーブルにするオプションを提供します。

ホストの接続インターフェイスが管理目的によってダウンしている場合、バインディングエントリは DOWN 状態になります。タイマーが設定されている場合、タイマーが切れる前にインターフェイスが再び稼働状態になる場合とエントリの DOWN 状態が維持される場合があります。タイマーが切れる前にインターフェイスが稼働状態になると、タイマーは停止し、エントリの状態が変化します。タイマーが切れた後もエントリの DOWN 状態が維持されると、そのエントリはバインディングテーブルから削除されます。タイマーがディセーブルまたはオフになっている場合、エントリはバインディングテーブルから削除されず、無期限に、またはインターフェイスが再び稼働状態になるまで、DOWN 状態が維持される可能性があります。

次のいずれかのオプションを設定します。

- **seconds**: ダウンライフタイムタイマーの値を設定します。1 ~ 86400 秒の値を入力します。デフォルト値は 86400 秒 (24 時間) です。
- **infinite**: DOWN 状態のタイマーをディセーブルにします。これは、エントリが DOWN 状態になったときにタイマーが開始されないことを意味します。

logging

バインディング エントリ イベントのログの生成をイネーブルにします。

**device-tracking
binding max-entries**
no_of_entries [
mac-limit *no_of_entries*
| **port-limit**
no_of_entries |
vlan-limit *no_of_entries*
]

バインディングテーブルのエントリの最大数を設定します。1 ~ 200000 の値を入力します。デフォルト値は 200000 です。

Note この制限は、ダイナミックエントリにのみ適用され、スタティック バインディング エントリには適用されません。

必要に応じて、次の制限を設定することもできます。

- **mac-limit no_of_entries**: 許可される MAC アドレスあたりの最大エントリ数を設定します。1 ~ 100000 の値を入力します。デフォルトでは、制限は設定されていません。
- **port-limit no_of_entries**: 許可されるインターフェイスあたりの最大エントリ数を設定します。1 ~ 100000 の値を入力します。デフォルトでは、制限は設定されていません。
- **vlan-limit no_of_entries**: 許可される VLAN あたりの最大エントリ数を設定します。1 ~ 100000 の値を入力します。デフォルトでは、制限は設定されていません。

このコマンドの **no** 形式を使用すると、**max-entries** 値が 200000 にリセットされ、**mac-limit**、**port-limit**、**vlan-limit** が「no limit」に設定されます。

reachable-lifetime { *seconds* | **infinite** } REACHABLE 状態のバインディングエントリのカウントダウンタイマーを設定するか、タイマーをディセーブルにするオプションを提供します。

タイマーが設定されている場合、タイマーが切れる前にホストから着信パケットを受信する場合とホストからの着信パケットがない場合があります。ホストから着信パケットを受信するたびに、タイマーがリセットされます。着信パケットを受信されずにタイマーが切れると、エントリの状態は、ホストの到達可能性に基づいて変化します。タイマーがディセーブルまたはオフになっている場合、エントリは無期限に REACHABLE 状態が維持される可能性があります。

次のいずれかのオプションを設定します。

- **seconds:** 到達可能ライフタイムタイマーの値を設定します。1～86400 秒の値を入力します。デフォルトは 300 秒（5 分）です。
- **infinite:** REACHABLE 状態のタイマーをディセーブルにします。これは、エントリが REACHABLE 状態になったときにタイマーが開始されないことを意味します。

stale-lifetime { *seconds* | **infinite** } STALE 状態のバインディングエントリのカウントダウンタイマーを設定するか、タイマーをディセーブルにするオプションを提供します。

タイマーが設定されている場合、タイマーが切れる前にホストから着信パケットを受信する場合とホストからの着信パケットがない場合があります。着信パケットを受信すると、タイマーが停止し、エントリは新しい状態に移行します。着信パケットを受信されずにタイマーが切れると、エントリはバインディングテーブルから削除されます。タイマーがディセーブルまたはオフになっている場合、エントリは無期限に STALE 状態が維持される可能性があります。

ポーリングがイネーブルになっている場合、ステイルタイマーが切れると、ホストをプローブする最後の試みが行われます。

Note ポーリングがイネーブルになっている場合、到達可能ライフタイムタイマーが切れるとポーリングが実行され（3 回）、その後、ステイルタイマーが切れると最後の試みも行われます。到達可能ライフタイムが切れた後のエントリのポーリングに必要な時間は、ステイルライフタイムから差し引かれます。

次のいずれかのオプションを設定します。

- **seconds:** ステイルライフタイム タイマーの値を設定します。1～86400 秒の値を入力します。デフォルト値は 86400 秒（24 時間）です。
- **infinite:** STALE 状態のタイマーをディセーブルにします。これは、エントリが STALE 状態になったときにタイマーが開始されないことを意味します。

```
device-tracking
binding vlan vlan_id
{ ipv4_add ipv6_add
  ipv6_prefix } {
interface
  inteface_type_no }
[
  48-bit-hardware-address
] [
reachable-lifetime {
  seconds | default |
infinite } tracking {
default | disable |
enable }
reachable-lifetime {
  seconds | default |
infinite } ]
```

バインディングテーブルのスタティック バインディング エントリを作成します。バインディングテーブルでスタティック バインディング エントリを維持する方法を指定することもできます。

Note 上記の **max-entries no_of_entries** オプションに設定する制限は、スタティックバインディング全体には適用されません。作成できるスタティックエントリの数に制限はありません。

- IP アドレスまたはプレフィックスを入力します。
 - **ipv4_add** : IPv4 アドレスを入力します。
 - **ipv6_add** : IPv6 アドレスを入力します。
 - **ipv6_prefix** : IPv6 プレフィックスを入力します。
- **interface interface_type_no**: インターフェイスのタイプと番号を入力します。デバイスで使用可能なインターフェイスのタイプを表示するには、疑問符 (?) のオンラインヘルプ機能を使用します。
- (任意) **48-bit-hardware-address**: MAC アドレスを入力します。バインディングエントリの MAC アドレスを設定しない場合、任意の MAC アドレスが許可されます。
- (任意) **reachable-lifetime {seconds | default | infinite }**: REACHABLE 状態のスタティック バインディング エントリの到達可能ライフタイムを設定します。スタティック バインディング エントリに到達可能ライフタイムを設定する場合は、エントリの MAC アドレスを指定する必要があります。

値を設定しない場合は、**device-tracking binding reachable-lifetime** に設定されている値が適用されます。

seconds: 到達可能ライフタイムタイマーの値を設定します。1～86400 秒の値を入力します。デフォルトは 300 秒 (5 分) です。

default: バインディングテーブルのダイナミックエントリに設定されている値を使用します。

infinite: REACHABLE 状態のタイマーをディセーブルにします。これは、スタティックバインディングエントリが REACHABLE 状態になったときにタイマーが開始されないことを意味します。

- (任意) **tracking {default | disable | enable}**: スタティック バインディング エントリのポーリング関連設定を指定します。

default: ポーリングはディセーブルになっています。

disable: スタティック バインディング エントリのポーリングをディセーブルにします。

enable: スタティックバインディングエントリのポーリングをイネー

ブルにします。

Command Default

値を設定しない場合、ポリシーレベルの値が設定されていないかぎり、ダウン、到達可能、およびステイルライフタイムのデフォルト値と、バインディングテーブルで許可されるバインディングエントリの最大数が適用されます。詳細については、「使用上のガイドライン」を参照してください。

Command Modes

グローバル コンフィギュレーション (Device(config)#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

device-tracking binding コマンドを使用すると、バインディングテーブルにおいてグローバルレベルでエントリを維持する方法を指定できます。これにより、設定は、SISF ベースのデバイストラッキングがイネーブルになっているすべてのインターフェイスおよび VLAN に適用されます。ただし、システムが、ネットワークに入るパケットからのバインディング情報の抽出を開始し、ここで指定した設定が適用されるバインディングエントリを作成するには、インターフェイスまたは VLAN にアタッチされたポリシーが存在する必要があります。

インターフェイスまたは VLAN にポリシーがない場合、バインディングテーブルに存在できるエントリは、作成したスタティック バインディング エントリだけです。

バインディングエントリ設定の変更

device-tracking binding コマンドを使用して値または設定を再指定すると、その変更は、その後に作成されたバインディングエントリにのみ適用されます。変更された設定は、既存のエントリには適用されません。古い設定は、古いエントリに適用されます。

現在の設定を表示するには、特権 EXEC モードで **show device-tracking database** コマンドを入力します。

グローバル設定とポリシーレベル設定

このコマンドで指定する設定の一部については、対応するものがポリシーレベルにもあります（ポリシーレベルのパラメータは、デバイストラッキング コンフィギュレーション モードで設定され、そのポリシーにのみ適用されます）。次の表に、グローバルに設定された値が優先される場合と、ポリシーレベルの値が優先される場合を示します。

グローバルコンフィギュレーションコマンドの device-tracking binding のオプション	デバイストラッキング コンフィギュレーション モードでのポリシーレベルの対応オプション
device-tracking binding reachable-lifetime { <i>seconds</i> infinite }	tracking enable [reachable-lifetime [<i>seconds</i> infinite]]
Device(config)# device-tracking binding reachable-lifetime 2000	Device(config)# device-tracking policy sisf-01 Device(config-device-tracking)# Device(config-device-tracking)# tracking enable reachable-lifetime 250

<p>グローバルコンフィギュレーションコマンドの device-tracking binding のオプション</p>	<p>デバイストラッキング コンフィギュレーションモードでのポリシーレベルの対応オプション</p>
<p>ポリシーレベルの値とグローバルに設定された値が存在する場合は、ポリシーレベルの値が適用されます。</p> <p>グローバルに設定された値のみが存在する場合、グローバルに設定された値が適用されます。</p> <p>ポリシーレベルの値のみが存在する場合、ポリシーレベルの値が適用されます。</p> <p>例: グローバルレベルとポリシーレベルで到達可能、ステイル、およびダウンライフタイムを設定する, on page 1428を参照してください。</p>	

<p>グローバルコンフィギュレーションコマンドの device-tracking binding のオプション</p>	<p>デバイストラッキング コンフィギュレーションモードでのポリシーレベルの対応オプション</p>
<p>device-tracking binding stale-lifetime { <i>seconds</i> infinite }</p>	<p>tracking disable [stale-lifetime [<i>seconds</i> infinite]]</p>
<pre>Device(config)# device-tracking binding stale-lifetime 2000</pre>	<pre>Device(config)# device-tracking policy sisf-01 Device(config-device-tracking)# Device(config-device-tracking)# tracking enable stale-lifetime 500</pre>
<p>ポリシーレベルの値とグローバルに設定された値が存在する場合は、ポリシーレベルの値が適用されます。</p> <p>グローバルに設定された値のみが存在する場合、グローバルに設定された値が適用されます。</p> <p>ポリシーレベルの値のみが存在する場合、ポリシーレベルの値が適用されます。</p> <p>例: グローバルレベルとポリシーレベルで到達可能、ステイル、およびダウンライフタイムを設定する, on page 1428を参照してください。</p>	

<p>グローバル コンフィギュレーション コマンドの device-tracking binding のオプション</p>	<p>デバイストラッキング コンフィギュレーションモードでのポリシーレベルの対応オプション</p>
<p>device-tracking binding max-entries <i>no_of_entries</i> [mac-limit <i>no_of_entries</i> port-limit <i>no_of_entries</i> vlan-limit <i>no_of_entries</i>]</p>	<p>limit address-count<i>tip-per-port</i></p>
<pre>Device(config)# device-tracking binding max-entries 30 vlan-limit 25 port-limit 20 mac-limit 19</pre>	<pre>Device(config)# device-tracking policy sisf-01 Device(config-device-tracking)# Device(config-device-tracking)# limit address-count 30</pre>

グローバル コンフィギュレーション コマンドの device-tracking binding のオプション	デバイストラッキング コンフィギュレーション モードでのポリシーレベルの対応オプション
<p>ポリシーレベルの値とグローバルに設定された値が存在する場合は、1つの制限（グローバル値またはポリシーレベルの値のいずれか）に達するとバインディングエントリの作成が停止します。</p> <p>グローバルに設定された値のみが存在する場合、1つの制限に達すると、バインディングエントリの作成が停止します。</p> <p>ポリシーレベルの値のみが存在する場合、ポリシーレベルの制限に達すると、バインディングエントリの作成が停止します。</p> <p>例: グローバルレベルのアドレス制限とポリシーレベルのアドレス制限, on page 1431.</p>	
グローバル コンフィギュレーション コマンドの device-tracking binding のオプション	デバイストラッキング コンフィギュレーション モードでのポリシーレベルの対応オプション
device-tracking binding max-entries <i>no_of_entries</i> [mac-limit <i>no_of_entries</i>]	MAC あたりの IPv4 および MAC あたりの IPv6 ポリシーでは上記の制限のどちらも設定できませんが、プログラムで作成されたポリシーでは、制限のいずれかまたは両方を設定することも、どちらも設定しないことも可能です。
<pre>Device(config)# device-tracking binding max-entries 300 mac-limit 3</pre>	<pre>Device# show device-tracking policy LISP-DT-GLEAN-VLAN Policy LISP-DT-GLEAN-VLAN configuration: security-level glean (*) device-role node gleaning from Neighbor Discovery gleaning from DHCP gleaning from ARP gleaning from DHCP4 NOT gleaning from protocol unkn limit address-count for IPv4 per mac 4 (*) limit address-count for IPv6 per mac 12 (*) tracking enable <output truncated></pre>
<p>ポリシーレベルの値とグローバルに設定された値が存在する場合は、1つの制限（グローバル値またはポリシーレベルの値のいずれか）に達するとバインディングエントリの作成が停止します。</p> <p>グローバルに設定された値のみが存在する場合、1つの制限に達すると、バインディングエントリの作成が停止します。</p> <p>ポリシーレベルの値のみが存在する場合、ポリシーレベルの制限に達すると、バインディングエントリの作成が停止します。</p>	

ダウン、到達可能、およびスタイルライフタイムの設定

down-lifetime、**reachable-lifetime**、または **stale-lifetime** キーワードにデフォルト以外の値を設定する場合、設定しないライフタイムはデフォルト値に戻されます。例：到達可能、ステイル、およびダウンライフタイムにデフォルト以外の値を設定する, on page 1427は、この動作が明確に示されている例です。

現在設定されているライフタイム値を表示するには、特権 EXEC モードで **show running-config | include device-tracking** コマンドを入力します。

MAC、ポート、および VLAN の制限の設定

mac-limit、**port-limit**、または **vlan-limit** キーワードにデフォルト以外の値を設定する場合、設定しない制限はデフォルト値に戻されます。

同じコマンドラインで3つの制限をすべて設定するには、最初に VLAN の制限、次にポートの制限、最後に MAC の制限を設定します。

```
Device(config)# device-tracking binding max-entries 15 vlan-limit 2 port-limit 20 mac-limit 5
```

このシステムの動作は、1つ以上（すべてではない）の制限をデフォルト値にリセットする場合にも使用できます。3つのキーワードはすべて、デフォルトが「制限なし」ですが、数値「0」を入力して制限をデフォルト値に設定することはできません。どの制限でも、0は有効な値の範囲に含まれていません。1つ以上の制限をデフォルト値にリセットするには、対応するキーワードを省略します。例：VLAN、ポート、およびMACの制限をデフォルト値に設定する, on page 1436は、この動作が明確に示されている例です。

バインディング エントリ イベントのロギングの設定

グローバル コンフィギュレーション コマンドの **device-tracking binding logging** を設定してバインディング エントリ イベントのログを生成する際、要件に応じて、いくつかの一般的なロギング設定も必要になる場合があります。

- (必須) グローバル コンフィギュレーション モードで **logging buffered informational** コマンドを使用します。

このコマンドを使用して、デバイスレベルでメッセージロギングをイネーブルにし、シビラティ（重大度）レベルを指定します。このコマンドの設定により、ログをコピーしてローカルの内部バッファに保存できます。シビラティレベルを指定すると、そのレベルのメッセージと、それより数値的に低いレベルのメッセージがログに記録されます。

バインディング エントリ イベントに関して生成されるログのシビラティレベルは6（つまり、情報）です。次に例を示します。

```
%SISF-6-ENTRY_CREATED: Entry created IP=192.0.2.24 VLAN=200 MAC=001b.4411.4ab6 I/F=Te1/0/4  
Preflevel=00FF
```

- (任意) グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。

このコマンドを使用して、ログをコンソール（使用可能なすべての TTY 回線）に送信します。



Caution シビラティレベルが低いと、コンソールに表示されるメッセージの数が大幅に増加する可能性があります。さらに、コンソールは表示が遅いデバイスです。メッセージストームでは、コンソールキューがいっぱいになると、一部のロギングメッセージがサイレント削除される場合があります。適切にシビラティレベルを設定してください。

このコマンドを設定しない場合は、特権 EXEC モードで **show logging** コマンドを入力することにより、必要に応じてログを表示できます。

logging console コマンドがイネーブルになっていない場合、ログはデバイスコンソールに表示されませんが、**device-tracking binding logging** および **logging buffered informational** が設定されている場合は、ログが生成され、ローカルバッファで使用できます。

ログが生成されるバインディングエントリ イベントの種類については、対応するリリースの [システムメッセージガイド](#) を参照してください。「SISF-6」を検索してください。

device-tracking binding logging コマンドはバインディング エントリ イベントをログに記録しますが、スヌーピングセキュリティ ロギングをイネーブルにする **device-tracking logging** コマンドもあります。2つのコマンドは異なる種類のイベントをログに記録し、生成されるログは異なるシビラティレベルを持ちます。

スタティック バインディング エントリの作成

レイヤ 2 ドメインにサイレントでも到達可能なホストがある場合、それらのサイレントホストのバインディング情報を保持するには、スタティック バインディング エントリを作成します。

作成できるスタティックエントリの数に制限はありませんが、これらのエントリはバインディングテーブルのサイズにも影響します。作成する前に、必要なスタティックエントリ数を考慮してください。

スタティック バインディング エントリで指定されたインターフェイスまたは VLAN にポリシーがアタッチされていない場合でも、スタティック バインディング エントリを作成できます。

スタティックバインディングエントリを設定するとき、その後に設定（たとえば、到達可能ライフタイム）を指定すると、その設定はそのスタティックバインディングエントリにのみ適用され、他のスタティックまたはダイナミックエントリには適用されません。例：[スタティック バインディング エントリを作成する, on page 1431](#) は、スタティック バインディング エントリを作成する例を示します。

例

- 例：到達可能、ステイル、およびダウンライフタイムにデフォルト以外の値を設定する, [on page 1427](#)
- 例：グローバルレベルとポリシーレベルで到達可能、ステイル、およびダウンライフタイムを設定する, [on page 1428](#)
- 例：スタティック バインディング エントリを作成する, [on page 1431](#)

- 例: グローバルレベルのアドレス制限とポリシーレベルのアドレス制限, on page 1431
- 例: VLAN、ポート、および MAC の制限をデフォルト値に設定する, on page 1436
- 例: MAC アドレスに関連するグローバルレベルの制限とポリシーレベルの制限, on page 1436

例: 到達可能、ステイル、およびダウンライフタイムにデフォルト以外の値を設定する

次の例には、到達可能、ステイル、およびダウンライフタイムの値を個別に設定した場合のシステムの動作が明確に示されています（影響は累積されません）。また、設定がすべてのライフタイムにわたって保持されるように値を設定する方法も示されています。

この例の最初のステップでは、到達可能ライフタイムのみが設定されます。**stale-lifetime** キーワードと **down-lifetime** キーワードが省略されているため、ダウンライフタイムとステイルライフタイムはデフォルトに設定されます。

```
Device(config)# device-tracking binding reachable-lifetime 700
Device(config)# exit
Device# show running-config | include device-tracking
device-tracking policy sisf-01
  device-tracking attach-policy sisf-01
  device-tracking attach-policy sisf-01 vlan 200device-tracking binding reachable-lifetime
700
device-tracking binding logging
```

この例の次のステップでは、ステイルライフタイムが 1500 秒、ダウンライフタイムが 1000 秒に設定されます。これにより、前のステップで設定された到達可能ライフタイムはデフォルトになります。

```
Device(config)# device-tracking binding stale-lifetime 1500 down-lifetime 1000
Device(config)# exit
Device# show running-config | include device-tracking
device-tracking policy sisf-01
  device-tracking attach-policy sisf-01
  device-tracking attach-policy sisf-01 vlan 200device-tracking binding stale-lifetime 1500
down-lifetime 1000
device-tracking binding logging
```

この例の次のステップでは、到達可能、ダウン、およびステイルライフタイムがそれぞれ 700、1000、および 200 に設定されます。これにより、ステイルライフタイムの値が 1500 秒から 1000 秒に変更されます。また、ダウンライフタイムが 1000 から 200 に変更されます。到達可能ライフタイムは 700 秒に設定されます。

```
Device(config)# device-tracking binding reachable-lifetime 700 stale-lifetime 1000
down-lifetime 200
Device(config)# exit
Device# show running-config | include device-tracking
device-tracking policy sisf-01
  device-tracking attach-policy sisf-01
  device-tracking attach-policy sisf-01 vlan 200device-tracking binding reachable-lifetime
700 stale-lifetime 1000 down-lifetime 200
device-tracking binding logging
```

いずれかのライフタイムを変更する必要があり、他のライフタイムの値を保持する必要がある場合は、毎回、同じコマンドラインを使用して、3 つのキーワードすべてを必要な値で再設定する必要があります。

例: グローバルレベルとポリシーレベルで到達可能、ステイル、およびダウンライフタイムを設定する

次に、グローバルレベルでバインディングエントリの到達可能、ステイル、およびダウンライフタイムを設定する例を示します。この例では、その後、ポリシーレベルの設定を指定することにより、グローバル設定を上書きし、特定のインターフェイスまたはVLANで学習されたエントリに異なるライフタイムを設定する方法も示しています。

この例の最初の部分において、**show device-tracking policy policy-name** コマンドの出力は、ポリシーレベルの値が設定されておらず、デフォルトのバインディングテーブル設定が既存のエントリに適用されることを示しています。グローバルコンフィギュレーションモードで**device-tracking binding** コマンドを使用して到達可能、ステイル、およびダウンライフタイムを設定すると、新しい値が有効になり、テーブルに追加された4つの新しいエントリにのみ適用されます。



Note **show device-tracking database** コマンドの出力のバインディングエントリに関する `Time left` 列に注意してください。各エントリの到達可能ライフタイムが、わずかに異なっています。これは、バインディングテーブルに多数のエントリが追加されるときにシステムパフォーマンスが低下しないようにシステムが課すジッター（設定値の +/-5%）です。バインディングエントリは時間をずらしてライフサイクルを通過するため、輻輳の発生が回避されます。

ポリシーレベルの到達可能ライフタイムが設定されていないことを示している、現在の設定です。バインディングテーブルエントリは、現在の到達可能ライフタイムが500秒（`Time left + age`）であることを示しています。

```
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy sisf-01 is applied on the following targets:
Target          Type  Policy          Feature          Target range
Tel1/0/4        PORT  sisf-01         Device-tracking  vlan 200

Device# show device-tracking database
Binding Table has 4 entries, 4 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned

Network Layer Address          Link Layer Address  Interface  vlan
prlvl   age      state      Time left          <<<<<
ARP 192.0.9.9                  000a.959d.6816     Tel1/0/4   200
0064   40s     REACHABLE  466 s              000a.959d.6816     Tel1/0/4   200
ARP 192.0.9.8                  000a.959d.6816     Tel1/0/4   200
0064   40s     REACHABLE  472 s              000a.959d.6816     Tel1/0/4   200
ARP 192.0.9.7                  000a.959d.6816     Tel1/0/4   200
0064   40s     REACHABLE  470 s
```

```
ARP 192.0.9.6          000a.959d.6816      Te1/0/4    200
0064          40s          REACHABLE  469 s
```

グローバルレベルでの到達可能、ステイル、およびダウンライフタイムの設定です。新しい値は、この後に作成されたバインディングエントリにのみ適用されます。

```
Device(config)# device-tracking binding reachable-lifetime 700 stale-lifetime 1000
down-lifetime 200
```

```
Device # show device-tracking database
```

```
Binding Table has 8 entries, 8 dynamic (limit 200000)
```

```
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
```

```
Preflevel flags (prlvl):
```

```
0001:MAC and LLA match      0002:Orig trunk      0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
```

Network Layer Address	prlvl	age	state	Time left	Link Layer Address	Interface	vlan
ARP 192.0.9.13	00C8	4s	REACHABLE	699 s	000a.959d.6816	Te1/0/4	200
					<<<< new global value applied		
ARP 192.0.9.12	00C8	4s	REACHABLE	719 s	000a.959d.6816	Te1/0/4	200
					<<<< new global value applied		
ARP 192.0.9.11	00C8	4s	REACHABLE	728 s	000a.959d.6816	Te1/0/4	200
					<<<< new global value applied		
ARP 192.0.9.10	00C8	4s	REACHABLE	712 s	000a.959d.6816	Te1/0/4	200
					<<<< new global value applied		
ARP 192.0.9.9	0064	9mn	STALE	try 0 1209 s	000a.959d.6816	Te1/0/4	200
ARP 192.0.9.8	0064	9mn	VERIFY	5 s try 3	000a.959d.6816	Te1/0/4	200
ARP 192.0.9.7	0064	9mn	VERIFY	2816 ms try 3	000a.959d.6816	Te1/0/4	200
ARP 192.0.9.6	0064	9mn	VERIFY	1792 ms try 3	000a.959d.6816	Te1/0/4	200

この例の2つ目の部分では、ポリシーレベルの値が設定されており、到達可能ライフタイムが50秒に設定されています。この新しい到達可能ライフタイムは、この後に作成されたエントリにのみ適用されます。

ポリシーレベルでは到達可能ライフタイムのみが設定され、ステイルライフタイムとダウンライフタイムは設定されません。これは、2つの新しいエントリの到達可能ライフタイムが切れ、STALE 状態または DOWN 状態に移行した場合に適用されるのが依然としてグローバル値であることを意味します。

```
Device(config)# device-tracking policy sisf-01
```

```
Device(config-device-tracking)# tracking enable reachable-lifetime 50
```

```
Device# show device-tracking policy sisf-01
```

```
Device-tracking policy sisf-01 configuration:
```

```
security-level guard
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP6
gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
```

```
tracking enable reachable-lifetime 50 <<<< new value applies only to binding entries
created after this and on interfaces and VLANs where this policy is attached.
```

```
Policy sisf-01 is applied on the following targets:
```

Target	Type	Policy	Feature	Target range
--------	------	--------	---------	--------------

```
Tel/0/4          PORT  sisf-01          Device-tracking vlan 200
```

```
Device# show device-tracking database
```

```
Binding Table has 10 entries, 10 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
```

Network Layer Address	prlvl	age	state	Time left	Link Layer Address	Interface	vlan
ARP 192.0.9.21					000a.959d.6816	Tel/0/4	200
0064	5s	REACHABLE	45 s		<<<< new policy-level value applied		
ARP 192.0.9.20					000a.959d.6816	Tel/0/4	200
0064	5s	REACHABLE	46 s		<<<< new policy-level value applied		
ARP 192.0.9.13					000a.959d.6816	Tel/0/4	200
00C8	14mn	STALE	try 0 865 s				
ARP 192.0.9.12					000a.959d.6816	Tel/0/4	200
00C8	14mn	STALE	try 0 183 s				
ARP 192.0.9.11					000a.959d.6816	Tel/0/4	200
00C8	14mn	STALE	try 0 178 s				
ARP 192.0.9.10					000a.959d.6816	Tel/0/4	200
00C8	14mn	STALE	try 0 165 s				
ARP 192.0.9.9					000a.959d.6816	Tel/0/4	200
0064	23mn	STALE	try 0 327 s				
ARP 192.0.9.8					000a.959d.6816	Tel/0/4	200
0064	23mn	STALE	try 0 286 s				
ARP 192.0.9.7					000a.959d.6816	Tel/0/4	200
0064	23mn	STALE	try 0 303 s				
ARP 192.0.9.6					000a.959d.6816	Tel/0/4	200
0064	23mn	STALE	try 0 306 s				

```
Device# show device-tracking database <<<< checking binding table again after new policy-level
reachable-lifetime expires
```

```
Binding Table has 7 entries, 7 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
```

Network Layer Address	prlvl	age	state	Time left	Link Layer Address	Interface	vlan
ARP 192.0.9.21					000a.959d.6816	Tel/0/4	200
0064	3mn	STALE	try 0 887 s		<<<< global value applies for stale-lifetime;		
					policy-level value was not configured		
ARP 192.0.9.20					000a.959d.6816	Tel/0/4	200
0064	3mn	STALE	try 0 884 s		<<<< global value applies for stale-lifetime;		
					policy-level value was not configured		
ARP 192.0.9.13					000a.959d.6816	Tel/0/4	200
00C8	17mn	STALE	try 0 664 s				
ARP 192.0.9.9					000a.959d.6816	Tel/0/4	200
0064	27mn	STALE	try 0 136 s				
ARP 192.0.9.8					000a.959d.6816	Tel/0/4	200
0064	27mn	STALE	try 0 96 s				
ARP 192.0.9.7					000a.959d.6816	Tel/0/4	200
0064	27mn	STALE	try 0 108 s				
ARP 192.0.9.6					000a.959d.6816	Tel/0/4	200
0064	27mn	STALE	try 0 111 s				

例: スタティック バインディング エントリを作成する

次に、スタティック バインディング エントリを作成する例を示します。エントリの先頭にある「S」は、スタティック バインディング エントリであることを示します。

```
Device(config)# device-tracking binding vlan 100 192.0.2.1 interface tengigabitethernet1/0/1
00:00:5e:00:53:af reachable-lifetime infinite
Device(config)# exit
Device# show device-tracking database
Binding Table has 2 entries, 0 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned

      Network Layer Address          Link Layer Address   Interface  vlan
prlvl  age      state      Time left          S   192.0.2.1
      0000.5e00.53af      Tel/0/1    100          0100      14s      REACHABLE
N/A
```

例: グローバルレベルのアドレス制限とポリシーレベルのアドレス制限

次に、グローバルレベルとポリシーレベルでアドレス制限を設定するときに、どちらのアドレス制限に達したのかを評価する例を示します。

グローバルレベルの設定は、次のコマンド文字列で設定された値を参照します。 **device-tracking binding max-entries no_of_entries [mac-limit no_of_entries | port-limit no_of_entries | vlan-limit no_of_entries]**

ポリシーレベルのパラメータは、デバイストラッキング コンフィギュレーション モードの **limit address-count** オプションを参照します。

この例の最初の部分では、次のように設定されています。

- グローバルレベルの設定: max-entries (最大エントリ数) = 30、vlan-limit (VLAN 制限) = 25、port-limit (ポート制限) = 20、mac-limit (MAC 制限) = 19
- ポリシーレベルの設定: limit address-count (アドレス数制限) = 45

特権 EXEC コマンドの **show device-tracking database details** の出力は、最初にポート制限 (max/port) に到達したことを示しています。ポートまたはインターフェイスでは、最大 20 のエントリが許可されます。これ以降、バインディングエントリは作成されません。MAC 制限に設定されている絶対値 (19) の方が低いですが、特権 EXEC コマンドの **show device-tracking database mac** の出力は、テーブルのバインディングエントリのリストに一意的 MAC アドレスが 3 つしかないことを示しています。したがって、この制限には達していません。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# device-tracking binding max-entries 30 vlan-limit 25 port-limit 20 mac-limit
19
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# limit address-count 45
Device(config-device-tracking)# end
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
```

```

security-level guard
device-role node
gleaning from Neighbor Discovery
gleaning from DHCP6
gleaning from ARP
gleaning from DHCP4
NOT gleaning from protocol unkn
limit address-count 45
Policy sisf-01 is applied on the following targets:
Target          Type Policy          Feature          Target range
Tel/0/4         PORT  sisf-01          Device-tracking vlan 200

```

Device# **show device-tracking database details**

```

Binding table configuration:
-----
max/box   : 30
max/vlan  : 25
max/port  : 20
max/mac   : 19

Binding table current counters:
-----
dynamic   : 20
local    : 0
total    : 20   <<<< no further entries created after this.

Binding table counters by state:
-----
REACHABLE : 20
  total   : 20
<output truncated>

```

Device# **show device-tracking database**

```

Binding Table has 20 entries, 20 dynamic (limit 30)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned

```

Network Layer	Address	prlvl	age	state	Time left	Link Layer Address	Interface	vlan
ARP	192.0.9.39					000c.959d.6816	Tel/0/4	200
	0064		14s	REACHABLE	37 s			
ARP	192.0.9.38					000b.959d.6816	Tel/0/4	200
	0064		14s	REACHABLE	37 s			
ARP	192.0.9.37					000b.959d.6816	Tel/0/4	200
	0064		14s	REACHABLE	36 s			
ARP	192.0.9.36					000b.959d.6816	Tel/0/4	200
	0064		14s	REACHABLE	39 s			
ARP	192.0.9.35					000b.959d.6816	Tel/0/4	200
	0064		14s	REACHABLE	38 s			
ARP	192.0.9.34					000b.959d.6816	Tel/0/4	200
	0064		14s	REACHABLE	37 s			
ARP	192.0.9.33					000b.959d.6816	Tel/0/4	200
	0064		15s	REACHABLE	36 s			
ARP	192.0.9.32					000b.959d.6816	Tel/0/4	200
	0064		15s	REACHABLE	37 s			
ARP	192.0.9.31					000b.959d.6816	Tel/0/4	200
	0064		15s	REACHABLE	36 s			
ARP	192.0.9.30					000b.959d.6816	Tel/0/4	200
	0064		15s	REACHABLE	36 s			
ARP	192.0.9.29					000b.959d.6816	Tel/0/4	200

```

0064      15s      REACHABLE  35 s
ARP 192.0.9.28
0064      15s      REACHABLE  36 s
ARP 192.0.9.27
0064      16s      REACHABLE  35 s
ARP 192.0.9.26
0064      16s      REACHABLE  36 s
ARP 192.0.9.25
0064      16s      REACHABLE  34 s
ARP 192.0.9.24
0064      16s      REACHABLE  35 s
ARP 192.0.9.23
0064      16s      REACHABLE  34 s
ARP 192.0.9.22
0064      16s      REACHABLE  36 s
ARP 192.0.9.21
0064      17s      REACHABLE  33 s
ARP 192.0.9.20
0064      17s      REACHABLE  33 s

```

```

Device# show device-tracking database mac
MAC                Interface  vlan      prlvl      state      Time left
Policy             Input_index
000c.959d.6816     Te1/0/4   200      NO TRUST   MAC-REACHABLE  27 s
sisf-01            12
000b.959d.6816     Te1/0/4   200      NO TRUST   MAC-REACHABLE  27 s
sisf-01            12
000a.959d.6816     Te1/0/4   200      NO TRUST   MAC-REACHABLE  27 s
sisf-01            12

```

この例の2つ目の部分では、次のように設定されています。

- グローバルレベルの設定: **max-entries** (最大エントリ数) = 30、**vlan-limit** (VLAN 制限) = 25、**port-limit** (ポート制限) = 20、**mac-limit** (MAC 制限) = 19
- ポリシーレベルの設定: **limit address-count** (アドレス数制限) = 14

最初に到達するのは、ポリシーレベルのアドレス数制限 (**limit address-count**) です。ポリシー「sisf-01」が適用されるポートまたはインターフェイスでは、最大 14 の IP アドレス (IPv4 および IPv6) が許可されます。これ以降、バインディングエントリは作成されません。MAC 制限に設定されている絶対値 (19) の方が低いですが、テーブルのバインディングエントリのリストには一意の MAC アドレスが 3 つしかありません。したがって、この制限には達していません。

```

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# limit address-count 14
Device(config-device-tracking)# end
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
 security-level guard
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP6
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
 limit address-count 14
Policy sisf-01 is applied on the following targets:
Target                Type  Policy                Feature                Target range

```

```
Tel/0/4          PORT  sisf-01          Device-tracking vlan 200
```

すべての既存エントリのステイルライフタイムが切れ、エントリがバインディングテーブルから削除された後、再設定された値に従って新しいエントリが追加されています。

```
Device# show device-tracking database <<<<checking time left for stale-lifetime to expire
for existing entries.
```

```
Binding Table has 20 entries, 20 dynamic (limit 30)
```

```
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
```

```
Preflevel flags (prlvl):
```

```
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
```

Network Layer	Address	prlvl	age	state	Time left	Link Layer Address	Interface	vlan
ARP	192.0.9.39					000c.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 316 s			
ARP	192.0.9.38					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 279 s			
ARP	192.0.9.37					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 308 s			
ARP	192.0.9.36					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 274 s			
ARP	192.0.9.35					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 279 s			
ARP	192.0.9.34					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 261 s			
ARP	192.0.9.33					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 258 s			
ARP	192.0.9.32					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 263 s			
ARP	192.0.9.31					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 266 s			
ARP	192.0.9.30					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 273 s			
ARP	192.0.9.29					000b.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 277 s			
ARP	192.0.9.28					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 282 s			
ARP	192.0.9.27					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 272 s			
ARP	192.0.9.26					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 268 s			
ARP	192.0.9.25					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 244 s			
ARP	192.0.9.24					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 248 s			
ARP	192.0.9.23					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 284 s			
ARP	192.0.9.22					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 241 s			
ARP	192.0.9.21					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 256 s			
ARP	192.0.9.20					000a.959d.6816	Tel/0/4	200
	0064		13mn	STALE	try 0 243 s			

```
Device# show device-tracking database <<<no output indicates no entries in the database
```

```
Device# show device-tracking database details
```

Binding table configuration:

```
-----
max/box : 30
max/vlan : 25
max/port : 20
max/mac : 19
```

Binding table current counters:

```
-----
dynamic : 14
local : 0
total : 14
```

Binding table counters by state:

```
-----
REACHABLE : 14
total : 14
<output truncated>
```

Device# **show device-tracking database**

Binding Table has 14 entries, 14 dynamic (limit 30)

Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created

Preflevel flags (prlvl):

```
0001:MAC and LLA match      0002:Orig trunk           0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access  0020:DHCP assigned
0040:Cga authenticated    0080:Cert authenticated   0100:Statically assigned
```

Network Layer	Address	prlvl	age	state	Time left	Link Layer Address	Interface	vlan
ARP	192.0.9.68					0001.5e00.53af	Te1/0/4	200
	0064		4s	REACHABLE	48 s			
ARP	192.0.9.67					0001.5e00.53af	Te1/0/4	200
	0064		4s	REACHABLE	48 s			
ARP	192.0.9.66					0001.5e00.53af	Te1/0/4	200
	0064		4s	REACHABLE	47 s			
ARP	192.0.9.65					0001.5e00.53af	Te1/0/4	200
	0064		4s	REACHABLE	48 s			
ARP	192.0.9.64					0001.5e00.53af	Te1/0/4	200
	0064		4s	REACHABLE	46 s			
ARP	192.0.9.63					0000.5e00.53af	Te1/0/4	200
	0064		7s	REACHABLE	44 s			
ARP	192.0.9.62					0000.5e00.53af	Te1/0/4	200
	0064		7s	REACHABLE	45 s			
ARP	192.0.9.61					0000.5e00.53af	Te1/0/4	200
	0064		7s	REACHABLE	43 s			
ARP	192.0.9.60					0000.5e00.53af	Te1/0/4	200
	0064		7s	REACHABLE	44 s			
ARP	192.0.9.59					0000.5e00.53af	Te1/0/4	200
	0064		7s	REACHABLE	44 s			
ARP	192.0.9.58					0000.5e00.53af	Te1/0/4	200
	0064		8s	REACHABLE	44 s			
ARP	192.0.9.57					0000.5e00.53af	Te1/0/4	200
	0064		8s	REACHABLE	44 s			
ARP	192.0.9.56					0000.5e00.53af	Te1/0/4	200
	0064		10s	REACHABLE	41 s			
ARP	192.0.9.55					0000.5e00.53af	Te1/0/4	200
	0064		10s	REACHABLE	40 s			

Device# **show device-tracking database mac**

MAC	Interface	vlan	prlvl	state	Time left
Policy	Input_index				
0001.5e00.53af	Te1/0/4	200	NO TRUST	MAC-REACHABLE	30 s
sisf-01	12				

```
0000.5e00.53af      Te1/0/4    200      NO TRUST  MAC-REACHABLE  30 s
sisf-01             12
```

例: VLAN、ポート、および MAC の制限をデフォルト値に設定する

次に、1 つ以上の制限をデフォルト値にリセットする例を示します。

```
Device(config)# device-tracking binding max-entries 30 vlan-limit 25 port-limit 20 mac-limit
19 <<<< all three limits configured.
Device(config)#exit
Device# show device-tracking database details
```

```
Binding table configuration:
-----
max/box   : 30
max/vlan  : 25
max/port  : 20
max/mac   : 19
<output truncated>
```

```
Device# configure terminal
Device(config)# device-tracking binding max-entries 30 vlan-limit 25 <<<< only VLAN limit
configured; port-limit and mac-limit keywords leftout.
Device(config)# exit
Device# show device-tracking database details
```

```
Binding table configuration:
-----
max/box   : 30
max/vlan  : 25
max/port  : no limit    <<<reset to default
max/mac   : no limit    <<<reset to default
```

例: MAC アドレスに関連するグローバルレベルの制限とポリシーレベルの制限

次の例は、グローバルレベルの MAC 制限とポリシーレベルの MAC 制限の優先順位がどのように決定されるのかを示しています。グローバル値は、許可される MAC アドレスあたりの最大エントリ数を指定します。プログラムポリシーでのみ設定可能なポリシーレベルの「MAC アドレスあたりの IPv4 制限」および「MAC アドレスあたりの IPv6 制限」により、許可される MAC アドレスあたりの IPv4 アドレス数および IPv6 アドレス数が指定されます。

この例の最初の部分では、グローバル値（MAC アドレスあたり 10 のエントリが許可される）が、ポリシーレベルの設定（MAC アドレスあたり 3 つの IPv4 アドレスが許可される）よりも高くなっています。特権 EXEC コマンドの **show device-tracking database details** の出力にある「Binding table current counters」（バインディングテーブルの現在のカウンタ）に、それが示されています。つまり、最初に到達するのはポリシーレベルの制限です。



Note どのポリシーでも、手動では「MAC アドレスあたりの IPv4 制限」や「MAC アドレスあたりの IPv6 制限」を設定できないため、ポリシーレベルの設定についての設定項目は表示されません。この例では、グローバルコンフィギュレーションモードで **ip dhcp snooping vlan vlan** コマンドを設定することにより、DT-PROGRAMMATIC ポリシーがターゲットに適用されています。プログラムで作成されるポリシーには、このパラメータに関する制限があるため、MAC アドレスあたりの IPv4 制限が存在します。

```

Device# configure terminal
Device(config)# ip dhcp snooping vlan 200
Device(config)# end
Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 3 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type      Policy          Feature          Target range
Tel/0/4     PORT     DT-PROGRAMMATIC Device-tracking  vlan 200

note:
Binding entry Down timer: 24 hours (*)
Binding entry Stale timer: 24 hours (*)

Device(config)# device-tracking binding max-entries 50 mac-limit 10
Device# show device-tracking database details
Binding table configuration:
-----
max/box   : 50
max/vlan  : no limit
max/port  : no limit
max/mac   : 10

Binding table current counters:
-----
dynamic   : 3
local     : 0
total     : 3

Binding table counters by state:
-----
REACHABLE : 2
total     : 3

Device# show device-tracking database
Binding Table has 3 entries, 3 dynamic (limit 50)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned

Network Layer Address      Link Layer Address      Interface  vlan  prlvl
  age      state      Time left
ARP 192.0.9.8              000a.959d.6816         Tel1/0/4  200  0064
   4s      REACHABLE  25 s
ARP 192.0.9.7              000a.959d.6816         Tel1/0/4  200  0064
   4s      REACHABLE  27 s
ARP 192.0.9.6              000a.959d.6816         Tel1/0/4  200  0064
  55s      VERIFY    5s try 2
<<<<<<policy-level limit reached; only up to 3 IPv4 addresses per MAC address are allowed.

Device# show device-tracking database mac

```

```

MAC                               Interface  vlan      prlvl      state      Time left
Policy                             Input_index
000a.959d.6816                   Tel/0/4   200       NO TRUST   MAC-STALE  93585 s
DT-PROGRAMMATIC                   12

```

この例の2つ目の部分では、グローバル値（MACアドレスあたり2つのエントリが許可される）が、ポリシーレベルの設定（MACアドレスあたり3つのIPv4アドレスが許可される）よりも低くなっています。特権EXECコマンドの**show device-tracking database details**の出力にある「Binding table current counters」（バインディングテーブルの現在のカウンタ）に、それが示されています。つまり、最初に到達するのはポリシーレベルの制限です。

```
Device# show device-tracking policy DT-PROGRAMMATIC
```

```

Policy DT-PROGRAMMATIC configuration:
 security-level glean (*)
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
 limit address-count for IPv4 per mac 3 (*)
 tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target   Type   Policy                Feature                Target range
Tel/0/4  PORT  DT-PROGRAMMATIC      Device-tracking        vlan 200

note:
Binding entry Down timer: 24 hours (*)
Binding entry Stale timer: 24 hours (*)

```

```
Device(config)# device-tracking binding max-entries 50 mac-limit 2
```

```
Device# show device-tracking database details
```

```

Binding table configuration:
-----
max/box   : 50
max/vlan  : no limit
max/port  : no limit
max/mac   : 2

Binding table current counters:
-----
dynamic   : 2
local     : 0
total     : 2

Binding table counters by state:
-----
REACHABLE : 2
total     : 2

```

```
Device# show device-tracking database
```

```

Binding Table has 3 entries, 3 dynamic (limit 50)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned

```

Network Layer Address				Link Layer Address	Interface	vlan	prlvl
age	state	Time left					
ARP 192.0.9.3				000a.959d.6816	Te1/0/4	200	0064
5s	REACHABLE	27 s					
ARP 192.0.9.4				000a.959d.6816	Te1/0/4	200	0064
6s	REACHABLE	20 s					

<<<<<global limit reached; only up to 2 binding entries per MAC address is allowed.

Device# **show device-tracking database mac**

MAC	Interface	vlan	prlvl	state	Time left
Policy	Input_index				
000a.959d.6816	Te1/0/4	200	NO TRUST	MAC-STALE	93585 s
DT-PROGRAMMATIC	12				

device-tracking logging

パケットドロップ、未解決パケット、MACまたはIP盗難の疑いなどのスヌーピングセキュリティイベントをログに記録するには、グローバル コンフィギュレーション モードで **device-tracking logging** コマンドを設定します。ロギングをディセーブルにするには、このコマンドの **no** 形式を入力します。

device-tracking logging [**packet drop** | **resolution-veto** | **theft**]

no device-tracking logging [**packet drop** | **resolution-veto** | **theft**]

Syntax Description

packet drop パケットドロップイベントをログに記録します。

resolution-veto 未解決パケットイベントをログに記録します。

theft IPおよびMAC盗難イベントをログに記録します。

Command Default

イベントはログに記録されません。

Command Modes

グローバル コンフィギュレーション (Device(config)#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スヌーピングセキュリティ イベントに関して生成されるログのシビラティ（重大度）レベルは4（つまり、警告）です。次に例を示します。

```
%SISF-4-PAK_DROP: Message dropped A=FE80::20D:FF:FE0E:F G=- V=10 I=Tu0 P=NDP::RA Reason=Packet not authorized on port
```

特権 EXEC モードで **show logging | include SISF-4** コマンドを入力すると、スヌーピングセキュリティ ログを表示できます。

ログが生成されるスヌーピングイベントの詳細については、対応するリリースの[システムメッセージガイド](#)を参照してください。「SISF-4」を検索してください。

パケットドロップイベント

packet drop キーワードを設定すると、パケットがドロップされるたびにログが生成されます。ログには、パケットドロップの理由も記載されます。この理由には次のものが含まれます（これらだけではありません）。

- Packet not authorized on port（ポートで認可されていないパケット）：これは、設定に基づいて、この種類のパケットがポートで予期されないため、セキュリティ機能によりパケットがドロップされたことを意味します。このようなセキュリティ機能とパケットがドロップされる状況の例としては、「ルータアドバタイズメントガード機能は、ルータ側ポートとして設定されていないポートで IPv6 ルータ アドバタイズメント パケットを受信した場合、そ

のパケットのドロップを決定することがある」や「DHCP ガード機能は、サーバー側ポートとして設定されていないポートでDHCPサーバーからのパケット（DHCP OFFERまたはDHCP REPLY）を受信した場合、そのパケットをドロップすることがある」などがあります（もちろん、これらだけではありません）。

- Packet accepted but not forwarded（受信されるが転送されないパケット）：これは、パケットは転送されないが、バインディング情報を収集するためにそのパケットが依然として有効であると見なされることを意味します。これは、通常、検証フェーズ中（バインディングが過渡的な状態にあるとき）にホストからのパケットがSISFによって認識されたときに見られます。
- Malformed Packet dropped in Guard mode（ガードモードでドロップされる不正な形式のパケット）：これは、着信パケットの形式が不正であり、正しく解析できないことを意味します。
- Packet is throttled（パケットがスロットルされる）：これは、時間間隔内にパケットのスロットリング制限を超えたためにパケットがドロップされたことを意味します。システムは、5秒間に最大50パケットを許可します。
- Silent drop（サイレントドロップ）：これは、デバイストラッキングインスタンスが、複数のスイッチにまたがる異なるインスタンス間で通信するために生成されたパケットか、デバイストラッキングによってトリガーされたアクションへの応答として生成されたパケットに対して発生します。たとえば、ホストの到達可能性のステータスを判断するためにデバイストラッキングによって開始されたプローブでの応答です。
- Martian packet（Martianパケット）：これは、着信パケットがMartian送信元IPアドレス（マルチキャスト、ループバック、または未指定のアドレスなど）を持っているためにドロップされたことを意味します。
- Martian mac（Martian MAC）：これは、着信パケットがMartian MACまたはリンク層の送信元アドレスを持っているためにドロップされたことを意味します。
- Address limit per box reached（ボックスあたりのアドレス制限に達した）：これは、グローバルコンフィギュレーションコマンドの **device-tracking binding max-entries no_of_entries** で設定された制限に達したために着信パケットがドロップされたことを意味します。現在の制限を表示するには、特権 EXEC コマンドの **show device-tracking database details** を入力します。
- Address limit per vlan reached（VLANあたりのアドレス制限に達した）：これは、グローバルコンフィギュレーションコマンドの **device-tracking binding max-entries no_of_entries vlan-limit no_of_entries** で設定された制限に達したために着信パケットがドロップされたことを意味します。現在の制限を表示するには、特権 EXEC コマンドの **show device-tracking database details** を入力します。
- Address limit per port reached（ポートあたりのアドレス制限に達した）：これは、グローバルコンフィギュレーションコマンドの **device-tracking binding max-entries no_of_entries port-limit no_of_entries** で設定された制限に達したために着信パケットがドロップされたことを意味します。現在の制限を表示するには、特権 EXEC コマンドの **show device-tracking database details** を入力します。

- Address limit per policy reached (ポリシーごとのアドレス制限に達した) : これは、デバイストラッキングコンフィギュレーションモードで **limit address-count ip-per-port** キーワードを使用して設定された制限に達したために着信パケットがドロップされたことを意味します。これはポリシーレベルで設定されます。現在の制限を表示するには、特権 EXEC コマンドの **show device-tracking policypolicy-name** を入力します。
- Address limit per mac reached (MAC あたりのアドレス制限に達した) : これは、グローバルコンフィギュレーションコマンドの **device-tracking binding max-entries no_of_entries mac-limit no_of_entries** で設定された制限に達したために着信パケットがドロップされたことを意味します。現在の制限を表示するには、特権 EXEC コマンドの **show device-tracking database details** を入力します。
- Address Family limit per mac reached (MAC あたりのアドレスファミリー制限に達した) : これは、プログラムポリシーで指定されたMACあたりのIPv4制限またはMACあたりのIPv6制限に達したために着信パケットがドロップされたことを意味します。このポリシーパラメータは設定できません。プログラムで作成されたポリシーには、MACあたりのIPv4制限とMACあたりのIPv6制限のいずれかまたはその両方が含まれる場合およびその両方が含まれない場合があります。制限が存在する場合、制限を表示するには、特権 EXEC コマンドの **show device-tracking policypolicy-name** を入力します。

解決拒否イベント

resolution-veto キーワードを設定すると、未解決パケットごとにログが生成されます。このログインゴプションは、IPv6 宛先ガード機能もイネーブルになっている場合にのみ使用することが意図されています。

IPv6 宛先ガード機能は、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレス解決を行うようにします。リンク上でアクティブなすべての宛先がバインディングテーブルに入力されます。バインディングテーブルに宛先が見つからない場合、アドレス解決は行われません。**resolution-veto** ログを設定することにより、このような未解決パケットを追跡できます。

resolution-veto キーワードが設定されていても、IPv6 宛先ガード機能が設定されていなければ、ログは生成されません。

盗難イベント

theft キーワードを設定すると、SISF が IP アドレスの盗難や MAC アドレスの盗難を検出したときにログが生成されます。

ログでは、検証されたバインディング情報 (IP、MAC アドレス、インターフェイス、VLAN) の前に「Known」という用語が付加されます。不審な IP アドレスおよび MAC アドレスの前には「New」または「Cand」という用語が付加されます。不審な IP アドレスまたは MAC アドレスとともにインターフェイスおよび VLAN 情報も提供されます。これは、不審なトラフィックがどこに現れたのかを特定するために役立ちます。

たとえば、次の MAC 盗難ログを参照してください。

```
%SISF-4-MAC_THEFT: MAC Theft Cand IP=2001::12B VLAN=70 MAC=9cfc.e85e.139d Cand I/F=Gil/0/4
Known IP=71.0.0.96 Known I/F=Ac0
```

このログに含まれる「Cand IP=2001::12B」、「VLAN=70」、および「Cand I/F=Gil/0/4」は、不審なホストの IP アドレスとそれが現れたインターフェイスを示しています。

このログに含まれる「MAC=9cfc.e85e.139d」は、不審なホストが使用している既知の MAC アドレスを示しています。

このログに含まれる「Known IP=71.0.0.96」および「Known I/F=Ac0」は、既存の検証済みエントリの IP アドレスおよびインターフェイスを示しています。

例

- 例: パケットドロップログ, on page 1443
- 例: 盗難ログ, on page 1443

例: パケットドロップログ

次に、パケットドロップイベントに関して生成されるログの例を示します。

```
%SISF-4-PAK_DROP: Message dropped A=FE80::20D:FF:FE0E:F G=- V=10 I=Tu0 P=NDP::RA Reason=Packet not authorized on port
```

```
%SISF-4-PAK_DROP: Message dropped A=20.0.0.1 M=dead.beef.0001 V=20 I=Gil/0/23 P=ARP Reason=Packet accepted but not forwarded
```

例: 盗難ログ

次に、IP 盗難イベントおよび MAC 盗難イベントに関して生成されるログの例を示します。

```
%SISF-4-MAC_AND_IP_THEFT: MAC_AND_IP Theft A=FE80::EE1D:8BFF:FE9B:102 V=102 I=Vl102 M=ec1d.8b9b.0102 New=Tu0
```

```
%SISF-4-MAC_THEFT: MAC Theft IP=192.2.1.2 VLAN=102 MAC=cafe.cafe.cafe I/F=Gil/0/3 New I/F over fabric
```

```
%SISF-4-IP_THEFT: IP Theft IP=FE80::9873:1D5E:E6E9:1F7E VLAN=20 MAC=2079.18d5.13ad IF=Ac0 New I/F over fabric
```

```
%SISF-4-IP_THEFT: IP Theft IP=10.0.187.5 VLAN=10 Cand-MAC=0069.0000.0001 Cand-I/F=Gil/0/23 Known MAC over-fabric Known I/F over-fabric
```

```
%SISF-4-MAC_THEFT: MAC Theft Cand IP=2001::12B VLAN=70 MAC=9cfc.e85e.139d Cand I/F=Gil/0/4 Known IP=71.0.0.96 Known I/F=Ac0
```

device-tracking policy

カスタムデバイストラッキングポリシーを作成し、デバイストラッキングコンフィギュレーションモードを開始してポリシーのさまざまなパラメータを設定するには、グローバルコンフィギュレーションモードで **device-tracking policy** コマンドを入力します。デバイストラッキングポリシーを削除するには、このコマンドの **no** 形式を使用します。

device-tracking policy *policy-name*
no device-tracking policy *policy-name*

Syntax Description

policy-name 指定された名前で作成されたデバイストラッキングポリシーを作成します（まだ存在しない場合）。プログラムで作成されたポリシーの名前を指定することもできます。

ポリシー名を設定すると、デバイスはデバイストラッキングコンフィギュレーションモードを開始し、ポリシーパラメータを設定できるようになります。設定可能なポリシーパラメータのリストを表示するには、システムプロンプトで疑問符(?)を入力します。

Command Default

SISF ベースのデバイストラッキングはディセーブルになっています。

Command Modes

グローバル コンフィギュレーション (Device(config)#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

グローバル コンフィギュレーションモードで **device-tracking policy***policy-name* コマンドを入力すると、システムは指定された名前で作成されたカスタムポリシーを作成し（まだ存在しない場合）、デバイストラッキングコンフィギュレーションモードを開始します。このモードでは、ポリシーパラメータを設定できます。

ポリシーを作成してそのパラメータを設定したら、それをインターフェイスまたは VLAN にアタッチする必要があります。その後には、ネットワークに入るパケットからバインディング情報 (IP および MAC アドレス) を抽出するアクティビティとバインディングエントリの作成が実際に開始されます。ポリシーのアタッチの詳細については、[device-tracking \(インターフェイスコンフィギュレーション\)](#), [on page 1410device-tracking \(VLAN コンフィギュレーション\)](#), [on page 1414](#) を参照してください。

デバイスで使用可能なすべてのポリシーとアタッチの対象に関する詳細情報を表示するには、特権 EXEC モードで **show device-tracking policies detail** コマンドを入力します。

ポリシーパラメータの設定

ポリシーのパラメータを設定できるのは、カスタムポリシーの場合のみです。プログラムポリシーのパラメータは変更できません。また、デフォルトポリシーのパラメータも変更できません。

ポリシーのパラメータのリストを表示するには、デバイストラッキング コンフィギュレーション モードのシステムプロンプトで疑問符 (?) を入力します。

```
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# ?
device-tracking policy configuration mode:
  data-glean          binding recovery by data traffic source address
                     gleaning
  default             Set a command to its defaults
  destination-glean  binding recovery by data traffic destination address
                     gleaning
  device-role        Sets the role of the device attached to the port
  distribution-switch Distribution switch to sync with
  exit               Exit from device-tracking policy configuration mode
  limit              Specifies a limit
  medium-type-wireless Force medium type to wireless
  no                 Negate a command or set its defaults
  prefix-glean       Glean prefixes in RA and DHCP-PD traffic
  protocol           Sets the protocol to glean (default all)
  security-level     setup security level
  tracking            Override default tracking behavior
  trusted-port       setup trusted port
  vpc                setup vpc port
```

キーワード	説明
data-glean	<p>ネットワーク内の送信元からスヌーピングされたデータパケットのアドレス学習をイネーブルにして、データトラフィックの送信元アドレスをバインディングテーブルに取り込みます。次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • log-only: データパケット通知時に syslog メッセージを生成します。 • recovery: プロトコルを使用してバインディングテーブルの回復をイネーブルにします。NDP または DHCP を入力します。

キーワード	説明
default	<p>ポリシーパラメータをデフォルト値に設定します。次のポリシー属性をデフォルト値に設定できます。</p> <ul style="list-style-type: none"> • data-glean: 送信元アドレスは学習または収集されません。 • destination-glean: 宛先アドレスは学習または収集されません。 • device-role: ノード。 • distribution-switch: サポートされていません。 • limit: アドレス数の制限は設定されません。 • medium-type-wireless: <tbid> • prefix-glean: プレフィックスは学習されません。 • protocol: すべてのプロトコル（ARP、DHCP4、DHCP6、NDP、およびUDP）のアドレスが収集されます。 • security-level: ガード。 • tracking: ポーリングはディセーブルになります。 • trusted-port: ディセーブルになります。つまり、設定されたターゲットでガード機能がイネーブルになります。 • vpc: サポートされていません。
destination-glean	<p>データトラフィックの宛先アドレスを収集して、バインディングテーブルの作成をイネーブルにします。次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • log-only: データパケット通知時に syslog メッセージを生成します。 • recovery: プロトコルを使用してバインディングテーブルの回復をイネーブルにします。NDPまたはDHCPを入力します。

キーワード	説明
device-role	<p>ポートに面するデバイスのタイプを示します。これは次のいずれかです。</p> <ul style="list-style-type: none"> • node: ポートのバインディングエントリの作成を許可します。 • switch: ポートのバインディングエントリの作成を停止します。このオプションは、大規模なデバイストラッキングテーブルの可能性が非常に高いマルチスイッチセットアップに適しています。このとき、デバイスに面するポート（アップリンクトランクポート）では、バインディングエントリの作成を停止するように設定できます。トランクポートの反対側のスイッチではデバイストラッキングがイネーブルにされ、バインディングエントリの有効性がチェックされるため、このようなポートに到着するトラフィックは信頼できます。 <p>このオプションは、通常、trusted-port キーワードとともに使用されます。アップリンクトランクポートで device-role オプションと trusted-port オプションの両方を設定すると、効率的で拡張可能な「セキュアゾーン」を構築できます。バインディングテーブルエントリの作成を効率的に分散させる（したがって、より小さなバインディングテーブルを保つ）ように、両方のパラメータを設定する必要があります。</p>
distribution-switch	このキーワードは、CLI のヘルプに表示されますが、サポートされていません。どの設定も有効になりません。
exit	デバイストラッキングコンフィギュレーションモードを終了して、グローバルコンフィギュレーションモードに戻ります。
limit address-count	<p>ポートごとに許可される IPv4 アドレスおよび IPv6 アドレスの最大数を設定します。この制限の目的は、バインディングエントリが既知のホストおよび予期されるホストのみに制限されるようにすることです。</p> <p>ip-per-port: ポートで許可する IP アドレスの最大数を入力します。この制限は、IPv4 アドレスと IPv6 アドレスの全体に適用されます。制限に達すると、バインディングテーブルに IP アドレスを追加できなくなり、新しいホストからのトラフィックはドロップされます。</p> <p>1 ~ 32000 の値を入力します。</p>
medium-type-wireless	このキーワードは、CLI のヘルプに表示されますが、サポートされていません。どの設定も有効になりません。

キーワード	説明
no	<p>コマンドを無効にします。つまり、ポリシーパラメータをデフォルト値に戻します。</p> <p>デフォルト値については、default キーワードを参照してください。</p> <ul style="list-style-type: none"> • data-glean • destination-glean • device-role • distribution-switch: サポートされていません。 • limit address-count • medium-type-wireless • prefix-glean • protocol • security-level • tracking • trusted-port • vpc: サポートされていません。
prefix-glean only	<p>IPv6 ルータアドバタイズメントまたは DHCP-PD のどちらかからのプレフィックスの学習をイネーブルにします。次のオプションがあります。</p> <p>(任意) only: プレフィックスのみを収集し、ホストアドレスは収集しません。</p>

キーワード	説明
protocol	<p>指定されたプロトコルのアドレスを収集します。デフォルトでは、すべてが収集されます。次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none">• arp [prefix-list name]: ARP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。• dhcp4 [prefix-list name]: DHCPv4 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。• dhcp6 [prefix-list name]: DHCPv6 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。• ndp [prefix-list name]: NDP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。• udp [prefix-list name]: このオプションは、CLI のヘルプに表示されますが、サポートされていません。どの設定も有効になりません。

キーワード	説明
security-level	<p>適用されるセキュリティのレベルを指定します。パケットがネットワークに入ると、SISFがIPアドレスとMACアドレス（パケットの送信元）を抽出します。後続のアクションは、ポリシーで設定されているセキュリティレベルによって決まります。</p> <p>次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • glean: IPアドレスとMACアドレスを抽出し、検証なしでバインディングテーブルに入力します。ホストについてのみ学習し、バインディングエントリの認証に関してSISFに依存しない場合は、このオプションを使用します。 • guard: IPアドレスとMACアドレスを抽出し、この情報をバインディングテーブルと照合します。検証の結果により、バインディングエントリが追加または更新されるか、またはパケットがドロップされてクライアントが拒否されるかが決まります。 <p>これは、セキュリティレベルパラメータのデフォルト値です。</p> <ul style="list-style-type: none"> • inspect: このキーワードはCLIで使用できますが、使用しないことを推奨します。上記のgleanおよびguardオプションは、ほぼすべての使用例とネットワーク要件に対応します。

キーワード	説明
tracking	<p>到達可能ライフタイムが切れた後にエントリがポーリングされるかどうかを決定します。ポーリングは、ホストの状態、まだ接続されているかどうか、および通信しているかどうかを確認するための、ホストの定期的な条件付きチェックです。ポーリングの詳細については、この後の「使用上のガイドライン」を参照してください。</p> <p>デフォルトでは、ポーリングはイネーブルになっていません。次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • disable : ポーリングアクションをオフにします。 <p>[stale-lifetime {seconds infinite}]: 必要に応じて、ステイルライフタイムを設定することもできます。その場合は、ステイルライフタイムタイマーに関して次のいずれかを設定します。</p> <ul style="list-style-type: none"> • seconds: ステイルライフタイムタイマーの値を設定します。1 ~ 86400 秒の値を入力します。デフォルト値は 86400 秒 (24 時間) です。 • infinite: STALE 状態のタイマーをディセーブルにします。これは、エントリが STALE 状態になったときにタイマーが開始されず、エントリが無期限に STALE 状態のままになることを意味します。 <ul style="list-style-type: none"> • enable: ポーリングアクションをオンにします。 <p>[reachable-lifetime [seconds infinite]]: 必要に応じて、到達可能ライフタイムを設定することもできます。その場合は、到達可能ライフタイムタイマーに関して次のいずれかを設定します。</p> <ul style="list-style-type: none"> • seconds: 到達可能ライフタイムタイマーの値を設定します。1 ~ 86400 秒の値を入力します。デフォルトは 300 秒 (5 分) です。 • infinite: REACHABLE 状態のタイマーをディセーブルにします。これは、エントリが REACHABLE 状態になったときにタイマーが開始されず、エントリが無期限に REACHABLE 状態のままになることを意味します。

キーワード	説明
trusted-port	<p>このオプションにより、設定されたターゲットでガード機能がディセーブルになります。trusted-port を経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。また、テーブル内にエントリーを作成しているときに衝突が発生した場合も、信頼できるポートが優先されます。</p> <p>このオプションは、通常、device-role キーワードとともに使用されます。アップリンクトランクポートで device-role オプションと trusted-port オプションの両方を設定すると、バインディングテーブルエントリーの作成を効率的に分散させる（したがって、より小さなバインディングテーブルを保つ）ことができます。</p>
vpc	このオプションは、CLI のヘルプに表示されますが、サポートされていません。どの設定も有効になりません。

グローバル設定とポリシーレベル設定

デバイストラッキングコンフィギュレーションモードでポリシーパラメータを設定します。ポリシーに関して設定した内容は、そのポリシーにのみ適用されます。一部のポリシーパラメータについては、グローバルコンフィギュレーションモードにも対応するパラメータがあります。グローバルレベルの対応するパラメータの詳細と、優先される値（グローバルに設定された値かポリシーレベルの値か）については、[device-tracking binding, on page 1417](#)を参照してください。

ホストのポーリング

tracking ポリシーパラメータを設定する場合、到達可能ライフタイムが切れると、スイッチがポーリング要求を送信します。スイッチは、システムが決定した固定の間隔で、最大3回ホストをポーリングします。また、グローバルコンフィギュレーションモードで **device-tracking tracking retry-interval seconds** コマンドを使用して間隔を指定することもできます。ポーリング要求は、Address Resolution Protocol (ARP) プロブまたはネイバー送信要求メッセージの形式です。この間、エントリーの状態は VERIFY に変わります。

ポーリング応答が受信されると（ホストの到達可能性が確認されると）、エントリーの状態は REACHABLE に戻ります。スイッチが3回試行してもポーリング応答を受信しない場合、エントリーは STALE 状態に変わります。



Note **tracking** ポリシーパラメータを使用すると、ポーリングがグローバルコンフィギュレーションレベルでイネーブルにされているかディセーブルにされているか（グローバルコンフィギュレーションモードの **device-tracking tracking** コマンド）に関係なく、ポリシーレベルでポーリングをイネーブルまたはディセーブルにできます。例：[ポリシーレベルでポーリングをディセーブルにする, on page 1453](#)および[device-tracking tracking, on page 1460](#)を参照してください。

アドレス数の制限の変更

limit address-count ポリシーパラメータを使用して制限を設定してから変更した場合、新しい制限は変更後に学習されたエントリにのみ適用されます。さらに、新しい制限が以前の制限より高いか低いかに関係なく、既存のエントリは影響を受けず、バインディングエントリのライフサイクルを通過できます。

バインディングテーブルがいっぱいになっている（以前の制限に従って）場合、既存のエントリがライフサイクルを完了するまで、新しいエントリは追加されません。SISFは、非アクティブエントリのみを識別して削除することにより、新しいエントリのためのスペースを作成しようとします。ただし、エントリがアクティブである場合、それらのエントリは削除されず、バインディングエントリのライフサイクルを通過できます。

低くした新しい制限をすぐに有効にするには、次のいずれかのオプションを使用できます。

- 特権 EXEC モードで **clear device-tracking database** コマンドを入力し、インターフェイスまたは VLAN を指定します。これにより、指定されたターゲットのデータベースのみから既存のすべてのエントリが削除されます。その後、新しいエントリが学習され、現在のアドレス数制限の設定に従って追加されます。例: [アドレス数の制限を変更する, on page 1454](#)を参照してください。
- 必要なターゲットでポリシーを削除して再アタッチします。ポリシーを削除するには、インターフェイスまたは VLAN コンフィギュレーションモードで **no device-tracking policypolicy-name** コマンドを入力します。インターフェイスまたは VLAN からポリシーを削除すると、ターゲットにアタッチされているバインディングが削除されます。それを再アタッチするには、インターフェイスまたは VLAN コンフィギュレーションモードで **device-tracking policypolicy-name** コマンドを入力します。ポリシーを再アタッチすると、新しい制限に従ってすべてのバインディングエントリが学習されます。

例

- 例: [ポリシーレベルでポーリングをディセーブルにする, on page 1453](#)
- 例: [アドレス数の制限を変更する, on page 1454](#)

例: ポリシーレベルでポーリングをディセーブルにする

次に、ポーリングがグローバルレベルでイネーブルになっている場合でも、ポリシーレベルでポーリングをディセーブルにする例を示します。ここでは、ポリシー `sisf-01` が適用されるすべてのインターフェイスおよび VLAN についてポーリングがディセーブルになっています。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# device-tracking tracking
Device(config)# exit
Device# show running-config | include device-tracking device-tracking tracking
device-tracking policy sisf-01
device-tracking attach-policy sisf-01
device-tracking attach-policy sisf-01 vlan 200
device-tracking binding reachable-lifetime 700 stale-lifetime 1000 down-lifetime 200
device-tracking binding logging
```

```

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# device-tracking policy sifs-01
Device(config-device-tracking)# tracking disable
Device(config-device-tracking)# end
Device# show device-tracking policy sifs-01
Device-tracking policy sifs-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 5
tracking disable
Policy sifs-01 is applied on the following targets:

```

Target	Type	Policy	Feature	Target range
Tel/0/4	PORT	sifs-01	Device-tracking	vlan 200
vlan 200	VLAN	sifs-01	Device-tracking	vlan all

例: アドレス数の制限を変更する

次に、**limit address-count** ポリシーパラメータ設定の変更をすぐに有効にする例を示します。この例では、変更した設定をすぐに有効にするために、**clear** コマンドを使用して、バインディングテーブルからすべてのエントリを削除します。

```

Device# show device-tracking policy sifs-01
Device-tracking policy sifs-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
limit address-count 25
Policy sifs-01 is applied on the following targets:

```

Target	Type	Policy	Feature	Target range
Tel/0/4	PORT	sifs-01	Device-tracking	vlan 200
vlan 200	VLAN	sifs-01	Device-tracking	vlan all

```

Device# show running-config | include device-tracking
device-tracking policy sifs-01
  device-tracking attach-policy sifs-01
  device-tracking attach-policy sifs-01 vlan 200
device-tracking binding reachable-lifetime 700 stale-lifetime 1000 down-lifetime 200
device-tracking binding logging

*Dec 13 15:08:50.723: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.25 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:08:50.723: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.26 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.27 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.28 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.29 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF

```

```
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.30 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.31 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.32 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.33 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.34 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.35 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.36 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.37 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.38 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.39 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.40 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.41 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.42 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.43 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_MAX_ORANGE: Reaching 80% of max adr allowed per policy
(25) V=200 I=Te1/0/4 M=001d.4411.3ab7
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.44 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.45 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.46 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.729: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.47 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.729: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.48 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.729: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.49 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
```

```
Device# show device-tracking database Binding Table has 25 entries, 25 dynamic (limit 20000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk           0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated   0100:Statically assigned
```

Network Layer Address				Link Layer Address	Interface	vlan
prlvl	age	state	Time left			
ARP	192.0.9.49			001d.4411.3ab7	Te1/0/4	200
	00FF	22s	REACHABLE	699 s		
ARP	192.0.9.48			001d.4411.3ab7	Te1/0/4	200
	00FF	22s	REACHABLE	691 s		
ARP	192.0.9.47			001d.4411.3ab7	Te1/0/4	200
	00FF	22s	REACHABLE	687 s		
ARP	192.0.9.46			001d.4411.3ab7	Te1/0/4	200
	00FF	22s	REACHABLE	714 s		
ARP	192.0.9.45			001d.4411.3ab7	Te1/0/4	200
	00FF	22s	REACHABLE	692 s		

```

ARP 192.0.9.44      00FF 22s REACHABLE 702 s 001d.4411.3ab7 Tel/0/4 200
ARP 192.0.9.43      00FF 22s REACHABLE 680 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.42      00FF 22s REACHABLE 708 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.41      00FF 22s REACHABLE 683 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.40      00FF 22s REACHABLE 708 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.39      00FF 22s REACHABLE 710 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.38      00FF 22s REACHABLE 697 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.37      00FF 22s REACHABLE 707 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.36      00FF 22s REACHABLE 695 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.35      00FF 22s REACHABLE 708 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.34      00FF 22s REACHABLE 706 s 001c.4411.3ab7 Tel/0/4 200
ARP 192.0.9.33      00FF 22s REACHABLE 683 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.32      00FF 22s REACHABLE 697 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.31      00FF 22s REACHABLE 683 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.30      00FF 22s REACHABLE 678 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.29      00FF 22s REACHABLE 696 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.28      00FF 22s REACHABLE 704 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.27      00FF 22s REACHABLE 713 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.26      00FF 22s REACHABLE 695 s 001b.4411.3ab7 Tel/0/4 200
ARP 192.0.9.25      00FF 22s REACHABLE 686 s 001b.4411.3ab7 Tel/0/4 200

```

アドレス数の制限が減らされて、25から5に変更されます。ただし、既存のエントリは、バインディングエントリのライフサイクルを完了していないため、バインディングテーブルから削除されません。新しいアドレス数の制限（5）をすぐに有効にするには、**clear device-tracking database** コマンドを使用して既存のエントリをすべて削除します。その後、新しいエントリが学習され、現在のアドレス数制限の設定に従って追加されます。

```

Device# configure terminal
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# limit address-count 5
Device(config-device-tracking)# end
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
 security-level guard
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP6
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
 limit address-count 5
Policy sisf-01 is applied on the following targets:

```

Target	Type	Policy	Feature	Target range
Tel/0/4	PORT	sisf-01	Device-tracking	vlan 200
vlan 200	VLAN	sisf-01	Device-tracking	vlan all

Device# **show device-tracking database**

Binding Table has 25 entries, 25 dynamic (limit 200000)

Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created

Preflevel flags (prlvl):

0001:MAC and LLA match	0002:Orig trunk	0004:Orig access
0008:Orig trusted trunk	0010:Orig trusted access	0020:DHCP assigned
0040:Cga authenticated	0080:Cert authenticated	0100:Statically assigned

prlvl	Network Layer Address	Link Layer Address	Interface	vlan
age	state	Time left		
ARP 192.0.9.49		001d.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	654 s		
ARP 192.0.9.48		001d.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	646 s		
ARP 192.0.9.47		001d.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	642 s		
ARP 192.0.9.46		001d.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	669 s		
ARP 192.0.9.45		001d.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	647 s		
ARP 192.0.9.44		001d.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	657 s		
ARP 192.0.9.43		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	635 s		
ARP 192.0.9.42		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	663 s		
ARP 192.0.9.41		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	638 s		
ARP 192.0.9.40		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	663 s		
ARP 192.0.9.39		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	665 s		
ARP 192.0.9.38		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	652 s		
ARP 192.0.9.37		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	662 s		
ARP 192.0.9.36		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	650 s		
ARP 192.0.9.35		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	663 s		
ARP 192.0.9.34		001c.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	661 s		
ARP 192.0.9.33		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	637 s		
ARP 192.0.9.32		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	652 s		
ARP 192.0.9.31		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	638 s		
ARP 192.0.9.30		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	633 s		
ARP 192.0.9.29		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	651 s		
ARP 192.0.9.28		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	658 s		
ARP 192.0.9.27		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	668 s		
ARP 192.0.9.26		001b.4411.3ab7	Tel1/0/4	200
00FF 67s	REACHABLE	650 s		

```
ARP 192.0.9.25          001b.4411.3ab7      Tel/0/4    200
00FF          67s          REACHABLE  641 s
```

```
Device# clear device-tracking database
```

```
*Dec 13 15:10:22.837: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.49 VLAN=200
MAC=001d.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.48 VLAN=200
MAC=001d.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.47 VLAN=200
MAC=001d.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.46 VLAN=200
MAC=001d.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.45 VLAN=200
MAC=001d.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.44 VLAN=200
MAC=001d.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.43 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.42 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.41 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.40 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.39 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.38 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.37 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.36 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.35 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.34 VLAN=200
MAC=001c.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.33 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.32 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.31 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.30 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.29 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.28 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.27 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.26 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.25 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
```

```
Device# show device-tracking database
```

```
<no output; binding table cleared>
```

```
*Dec 13 15:11:38.346: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.25 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:11:38.346: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.26 VLAN=200
MAC=001b.4411.3ab7 I/F=Tel/0/4 Preflevel=00FF
*Dec 13 15:11:38.347: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.27 VLAN=200
```

```

MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:11:38.347: %SISF-6-ENTRY_MAX_ORANGE: Reaching 80% of max adr allowed per policy
(5) V=200 I=Te1/0/4 M=001b.4411.3ab7
*Dec 13 15:11:38.347: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.28 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:11:38.347: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.29 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF

```

Device# **show device-tracking database**

```

Binding Table has 5 entries, 5 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned

```

prlvl	Network Layer Address	age	state	Time left	Link Layer Address	Interface	vlan
ARP	192.0.9.29	15s	REACHABLE	716 s	001b.4411.3ab7	Te1/0/4	200
00FF							
ARP	192.0.9.28	15s	REACHABLE	702 s	001b.4411.3ab7	Te1/0/4	200
00FF							
ARP	192.0.9.27	15s	REACHABLE	705 s	001b.4411.3ab7	Te1/0/4	200
00FF							
ARP	192.0.9.26	15s	REACHABLE	716 s	001b.4411.3ab7	Te1/0/4	200
00FF							
ARP	192.0.9.25	15s	REACHABLE	718 s	001b.4411.3ab7	Te1/0/4	200
00FF							

device-tracking tracking

IPv4 および IPv6 のポーリングをイネーブルにして、ポーリングパラメータを設定するには、グローバル コンフィギュレーション モードで **device-tracking tracking** コマンドを設定します。ポーリングをディセーブルにするには、このコマンドの **no** 形式を入力します。



Note このコマンドは、SISF ベースのデバイストラッキング機能をイネーブルにしません。これにより、デバイストラッキング機能がイネーブルになっているデバイスでのポーリングパラメータの設定が可能になります。

```
device-tracking tracking [ auto-source [ fallback ipv4_and_fallback_source_mask ip_prefix_mask [
override ] | retry-interval seconds ]
```

```
no device-tracking tracking [ auto-source | retry-interval ]
```

Syntax Description

auto-source

Address Resolution Protocol (ARP) プローブの送信元アドレスが、次の優先順位で使用されるようにします。

- 第 1 の優先事項は、SVI が設定されている場合に、送信元アドレスを VLAN SVI に設定することです。
- 第 2 の優先事項は、同じサブネットからデバイストラッキングテーブル内の IP-MAC バインディングエントリを見つけ、それを送信元アドレスとして使用することです。
- 第 3 かつ最後の優先事項は、送信元アドレスとして 0.0.0.0 を使用することです。

fallback ARP プローブの送信元アドレスが、次の優先順位で使用されるようにします。
ipv4_and_fallback_source_maskip_prefix_mask

- 第1の優先事項は、SVI が設定されている場合に、送信元アドレスを VLAN SVI に設定することです。
- 第2の優先事項は、同じサブネットからデバイストラッキングテーブル内の IP-MAC バインディングエントリを見つけ、それを送信元アドレスとして使用することです。
- 第3かつ最後の優先事項は、クライアントの IPv4 アドレスおよび提供されたマスクから送信元アドレスを計算することです。

送信元 MAC アドレスは、クライアント側のスイッチポートの MAC アドレスから取得されます。

fallback キーワードを設定する場合は、IP アドレスとマスクも指定する必要があります。

override ARP プローブの送信元アドレスが、次の優先順位で使用されるようにします。

- 第1の優先事項は、VLAN SVI が設定されている場合に、送信元アドレスを VLAN SVI に設定することです。
- 第2かつ最後の優先事項は、送信元アドレスとして 0.0.0.0 を使用することです。

Note このキーワードにより、SISF がバインディングテーブルから送信元アドレスを選択しないように設定されます。SVI が設定されていない場合、このオプションを使用することは推奨されません。

retry-interval seconds

バックオフアルゴリズムの乗算係数または「基本値」を設定します。バックオフアルゴリズムにより、到達可能ライフタイムが切れた後に3回試行されるポーリングの間の待機時間が決定されます。

1～3600秒の値を入力します。デフォルト値は1です。

ポーリング時には、3回のポーリング試行または再試行の間の待機時間は増加します。バックオフアルゴリズムにより、この待機時間が決定されます。再試行間隔に設定した値は、バックオフアルゴリズムの待機時間で乗算されます。

たとえば、バックオフアルゴリズムにより3回の試行の間でそれぞれ2、4、および6秒の待機時間が決定され、再試行間隔を2秒に設定した場合、観測される実際の間隔は、最初のポーリング試行までの待機時間が2 X 2秒、2回目のポーリング試行までの待機時間が2 X 4秒、3回目のポーリング試行までの待機時間が2 X 6秒になります。

ポーリングがイネーブルになっているのに再試行間隔が設定されていない場合、スイッチは、システムによって決定される間隔で最大3回ホストをポーリングします。

この設定は、ARPプローブとネイバー送信要求メッセージに適用されます。

Command Default

ポーリングは、デフォルトではディセーブルになっています。

Command Modes

グローバル コンフィギュレーション (Device(config)#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ポーリングは、ホストの状態、まだ接続されているかどうか、および通信しているかどうかを確認するための、ホストの定期的な条件付きチェックです。ポーリングにより、トラッキング対象デバイスの継続的な存在を評価できます。

ポーリングは、到達可能ライフタイムタイマーが切れた後に3回試行され、ステイルライフタイムが切れるときに最後の1回試行されます。

- IPv4ネットワークでは、ポーリングはARPプローブの形式です。この場合、スイッチは、接続されたホストにユニキャストARPプローブを送信して、ホストの到達可能性ステータスを判別します。ARPプローブを送信する場合、システムは、RFC 5227仕様に従ってパケットを構築します。

- IPv6 ネットワークでは、ポーリングはネイバー送信要求メッセージの形式です。この場合、スイッチは、接続されたホストのユニキャストアドレスを宛先アドレスとして使用して、接続されたホストの到達可能性を検証します。

IPv4 および IPv6 のポーリングをイネーブルにするには、グローバルコンフィギュレーションモードで **device-tracking tracking** コマンドを設定します。

また、到達可能ライフタイムタイマーが切れた後のポーリング間隔を設定するには、**retry-interval seconds** も設定します。



Note **auto-source** キーワード、**fallback ipv4_and_fallback_source_maskip_prefix_mask** キーワード、および **override** キーワードは、ARP プロンプトにのみ適用され、ネイバー送信要求メッセージには適用されません。

retry-interval seconds キーワードに設定する値は、IPv4 と IPv6 の両方に適用されます。

現在のポーリング設定を表示するには、**show running-config | include device-tracking** を入力します。次に例を示します。

```
Device# show running-config | include device-tracking
device-tracking tracking retry-interval 2
device-tracking policy sisf-01
  device-tracking attach-policy sisf-01 vlan 200
device-tracking binding reachable-lifetime 50 stale-lifetime 150 down-lifetime 30
device-tracking binding logging
```

エントリのさまざまなライフタイムの期間を表示するには、特権 EXEC モードで **show device-tracking database** コマンドを入力します。ポーリング中に、システムは、エントリの状態を VERIFY に変更します。期間を観測するには、出力の Time left 列を調べます。

show device-tracking database コマンドを使用してエントリの到達可能ライフタイムとステイルライフタイムをトラッキングし、ポーリングをイネーブルにすると、ステイルライフタイムが設定よりも短いことに気付く場合があります。これは、ポーリングに必要な時間がステイルライフタイムから差し引かれるためです。

ポーリングのグローバル設定とポリシーレベル設定

グローバルコンフィギュレーションモードで **device-tracking tracking** コマンドを設定した後も、個々のインターフェイスおよび VLAN で、ポーリングを柔軟にオンまたはオフにできます。このためには、ポリシーでポーリングを有効または無効にする必要があります。グローバル設定とポリシーレベル設定がどのように相互作用するのかに注意してください。

グローバル設定	ポリシーレベル設定	結果
ポーリングをグローバルレベルでイネーブルにします。 Device(config)# device-tracking tracking	インターフェイスまたはVLANでポーリングをイネーブルにします。 Device(config-device-tracking)# tracking enable	インターフェイスまたはVLANでポーリングが有効になります。
	インターフェイスまたはVLANでポーリングをディセーブルにします。 Device(config-device-tracking)# tracking disable	インターフェイスまたはVLANでポーリングは有効になりません。
	インターフェイスまたはVLANでデフォルトのポーリングを設定します。 Device(config-device-tracking)# default tracking	ポーリングがグローバルコンフィギュレーションレベルでイネーブルになっているため、ポーリングはインターフェイスまたはVLANで有効になります。
	インターフェイスまたはVLANでこのコマンドの no 形式を設定します。 Device(config-device-tracking)# no tracking	コマンドの no 形式を使用すると、コマンドがデフォルト値に設定されます。ただし、ポーリングがグローバルコンフィギュレーションレベルでイネーブルになっているため、ポーリングはインターフェイスまたはVLANで有効になります。

グローバル設定	ポリシーレベル設定	結果
<p>ポーリングをグローバルレベルでディセーブルにします。</p> <pre>Device(config)# no device-tracking tracking</pre>	<p>インターフェイスまたはVLANでポーリングをイネーブルにします。</p> <pre>Device(config-device-tracking)# tracking enable</pre>	<p>インターフェイスまたはVLANでポーリングが有効になります。</p>
	<p>インターフェイスまたはVLANでポーリングをディセーブルにします。</p> <pre>Device(config-device-tracking)# tracking disable</pre>	<p>インターフェイスまたはVLANでポーリングは有効になりません。</p>
	<p>インターフェイスまたはVLANでデフォルトのポーリングを設定します。</p> <pre>Device(config-device-tracking)# default tracking</pre>	<p>インターフェイスまたはVLANでポーリングは有効になりません。</p>
	<p>インターフェイスまたはVLANでこのコマンドの no 形式を設定します。</p> <pre>Device(config-device-tracking)# no tracking</pre>	<p>インターフェイスまたはVLANでポーリングは有効になりません。</p>

device-tracking upgrade-cli

レガシー IP デバイストラッキング (IPDT) および IPv6 スヌーピングコマンドを SISF コマンドに変換するには、グローバル コンフィギュレーション モードで **device-tracking upgrade-cli** コマンドを設定します。レガシーコマンドに戻すには、このコマンドの **no** 形式を入力します。

device-tracking upgrade-cli [**force** | **revert**]

no device-tracking upgrade-cli [**force** | **revert**]

Syntax Description	force 確認手順をスキップし、レガシー IPDT および IPv6 スヌーピングコマンドを SISF コマンドに変換します。
	revert レガシー IPDT および IPv6 スヌーピングコマンドに戻します。
Command Default	レガシー IPDT および IPv6 スヌーピングコマンドは、そのまま残ります。
Command Modes	グローバル コンフィギュレーション (Device(config)#)
Command History	リリース 変更内容 Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

デバイスにあるレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドは CLI を異なる方法でアップグレードします。既存の設定を移行する前に、次の設定シナリオ、および対応する移行結果を検討します。



Note 古い IPDT と IPv6 スヌーピング CLI を SISF ベースのデバイストラッキング CLI と併用することはできません。

IPDT 設定のみが存在する

デバイスに IPDT 設定のみがある場合は、**device-tracking upgrade-cli** コマンドを実行すると、設定が変換され、新しく作成されてインターフェイスで適用される SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

引き続きレガシーコマンドを使用する場合、レガシーモードでの操作に制限されます。このモードでは、レガシー IPDT と IPv6 スヌーピングコマンドのみがデバイスで使用可能になります。

IPv6 スヌーピング設定のみが存在する

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピングコマンドを以降の設定に使用できます。次のオプションを使用できます。

- (推奨) **device-tracking upgrade-cli** コマンドを使用して、レガシー設定をすべて、新しい SISF ベースのデバイストラッキング コマンドに変換します。変換後は、新しいデバイストラッキング コマンドのみがデバイスで動作します。
- レガシー IPv6 スヌーピングコマンドを今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しません。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピングコマンドのみであり、新しい SISF ベースのデバイストラッキング CLI コマンドは使用できません。

IPDT と IPv6 スヌーピングの両方の設定が存在する

レガシー IPDT 設定と IPv6 スヌーピング設定の両方が存在するデバイスでは、レガシーコマンドを SISF ベースのデバイストラッキング CLI コマンドに変換できます。ただし、インターフェイスに適用することができるスヌーピングポリシーは1つだけであり、IPv6 スヌーピングポリシーパラメータは IPDT 設定よりも優先される、ということに注意してください。



Note 新しい SISF ベースのコマンドに移行しておらず、レガシー IPv6 スヌーピングや IPDT コマンドを使用し続けている場合、IPv4 デバイストラッキング設定情報が IPv6 スヌーピングコマンドに表示される可能性があります。SISF ベースのデバイストラッキング機能では、IPv4 と IPv6 の両方の設定を扱うためです。これを回避するには、レガシー設定を SISF ベースのデバイストラッキング コマンドに変換することを推奨します。

IPDT または IPv6 スヌーピング設定が存在しない

デバイスにレガシー IP デバイストラッキング設定も IPv6 スヌーピング設定もない場合は、今後の設定に使用できるのは新しい SISF ベースのデバイストラッキング コマンドのみです。レガシー IPDT コマンドと IPv6 スヌーピングコマンドは使用できません。

例

次に、IPv6 スヌーピングコマンドを SISF ベースのデバイストラッキング コマンドに変換する例を示します。

```
Device# show ipv6 snooping features
Feature name  priority state
Device-tracking  128  READY
Source guard   32   READY

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking upgrade-cli
 IPv6 Snooping and IPv4 device tracking CLI will be
 converted to the new top level device-tracking CLI
Are you sure ? [yes]: yes
Number of Snooping Policies Upgraded: 2
Device(config)# exit
```

変換後、新しい SISF ベースのデバイストラッキング コマンドのみがデバイスで動作します。

```
Device# show ipv6 snooping features
      ^
% Invalid input detected at '^' marker.

Device# show device-tracking features
Feature name  priority state
Device-tracking  128  READY
Source guard   32   READY

Device# show device-tracking policies
Target                Type  Policy                Feature          Target range
Tel/0/4                PORT  sif-01                Device-tracking  vlan 200
vlan 200                VLAN  sif-01                Device-tracking  vlan all
```

dnscrypt (パラメータマップ)

シスコデバイスと Cisco Umbrella 統合機能の間の通信を認証するためにドメインネームシステム (DNS) パケット暗号化をイネーブルにするには、パラメータマップタイプ検査コンフィギュレーションモードで **dnscrypt** コマンドを使用します。DNS パケット暗号化をディセーブルにするには、このコマンドの **no** 形式を使用します。

dnscrypt
no dnscrypt

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

Umbrella モードの DNS パケット暗号化は設定されていません。

Command Modes

パラメータマップタイプ検査コンフィギュレーション (config-profile)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines

DNSCrypt を使用する場合は、DNS 要求パケットサイズが 512 バイトよりも大きくなります。これらのパケットが中間デバイスで許可されていることを確認します。そうしないと、応答が目的の受信者に到達しない可能性があります。

Examples

次に、DNS パケット暗号化をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)# dnscrypt
```

Related Commands

コマンド	説明
parameter-map type umbrella global	Umbrella モードでパラメータマップタイプを設定します。

dot1x critical (グローバル コンフィギュレーション)

IEEE 802.1X クリティカル認証パラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。

dot1x critical eapol

Syntax Description	eapol デバイスがクリティカルポートを正常に認証すると、スイッチがEAPOL成功メッセージを送信するように指定します。				
Command Default	eapol はディセーブルです				
Command Modes	グローバル コンフィギュレーション (config)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

次に、デバイスがクリティカルポートを正常に認証すると、デバイスがEAPOL成功メッセージを送信するように指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x critical eapol
Device(config)# exit
```

dot1x logging verbose

802.1X システムメッセージから詳細情報をフィルタリングするには、デバイススタックまたはスタンドアロンデバイス上で **dot1x logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

dot1x logging verbose
no dot1x logging verbose

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

システムメッセージの詳細ログは有効になっていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドにより、802.1X システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

次に、verbose 802.1X システムメッセージをフィルタリングする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x logging verbose
Device(config)# exit
```

Related Commands

コマンド	説明
authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングする
dot1x logging verbose	802.1X システムメッセージから詳細情報をフィルタリングする
mab logging verbose	MAC 認証バイパス (MAB) システムメッセージから詳細情報をフィルタリングする

dot1x pae

Port Access Entity (PAE) タイプを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。設定された PAE タイプをディセーブルにするには、コマンドの **no** 形式を入力します。

```
dot1x pae {supplicant | authenticator}
no dot1x pae {supplicant | authenticator}
```

Syntax Description

supplicant インターフェイスはサブリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。

authenticator インターフェイスはオーセンティケータとしてだけ動作し、サブリカント向けのメッセージに応答しません。

Command Default

PAE タイプは設定されていません。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

IEEE 802.1X 認証をポート上でディセーブルにする場合は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

dot1x port-control インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1X 認証を設定した場合、デバイスは自動的にポートを IEEE 802.1X オーセンティケータとして設定します。オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

次に、インターフェイスがサブリカントとして動作するように設定されている例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x pae supplicant
Device(config-if)# end
```

dot1x supplicant controlled transient

認証中に 802.1X サプリカントポートへのアクセスを制御するには、グローバルコンフィギュレーションモードで **dot1x supplicant controlled transient** コマンドを使用します。認証中にサプリカントのポートを開くには、このコマンドの **no** 形式を使用します。

dot1x supplicant controlled transient
no dot1x supplicant controlled transient

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

認証中に 802.1X サプリカントのポートへのアクセスが許可されます。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デフォルトでは、BPCU ガードがイネーブルにされたオーセンティケータスイッチにサプリカントのデバイスを接続する場合、オーセンティケータのポートはサプリカントスイッチが認証する前にスパンニングツリープロトコル (STP) のブリッジプロトコルデータユニット (BPDU) を受信した場合、**errdisable** 状態になる可能性があります。認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** コマンドを入力すると、認証が完了する前にオーセンティケータポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートがブロックされます。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** コマンドを入力すると、認証期間中にサプリカントポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータスイッチポートでイネーブルになっている場合、サプリカントデバイスで **dot1x supplicant controlled transient** コマンドを使用することを推奨します。

次に、認証の間にデバイスの 802.1X サプリカントのポートへのアクセスを制御する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x supplicant controlled transient
Device(config)# exit
```

dot1x supplicant force-multicast

サブリカントスイッチでマルチキャストまたはユニキャストの Extensible Authentication Protocol over LAN (EAPOL) パケットを受信した場合に、常にマルチキャスト EAPOL パケットのみを送信するように強制するには、グローバル コンフィギュレーション モードで **dot1x supplicant force-multicast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x supplicant force-multicast
no dot1x supplicant force-multicast

Syntax Description このコマンドには、引数またはキーワードはありません。

Command Default サブリカントデバイスは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines Network Edge Access Topology (NEAT) がすべてのホストモードで機能するようにするには、サブリカントデバイス上でこのコマンドをイネーブルにします。

次の例では、サブリカントデバイスがオーセンティケータデバイスにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x supplicant force-multicast
Device(config)# end
```

Related Commands

コマンド	説明
cisp enable	デバイス上で CISP をイネーブルにタとして機能するようにします。
dot1x credentials	ポートに 802.1X サブリカントのク
dot1x pae supplicant	インターフェイスがサブリカントと

dot1x test eapol-capable

すべてのスイッチポート上の IEEE 802.1X のアクティビティをモニタリングして、IEEE 802.1X をサポートするポートに接続しているデバイスの情報を表示するには、特権 EXEC モードで **dot1x test eapol-capable** コマンドを使用します。

dot1x test eapol-capable [**interface** *interface-id*]

Syntax Description	interface <i>interface-id</i>	(任意) クエリー対象のポートです。
Command Default	デフォルト設定はありません。	
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1X 機能をテストするには、このコマンドを使用します。

このコマンドには、no 形式はありません。

次の例では、スイッチ上で IEEE 802.1X の準備チェックをイネーブルにして、ポートに対してクエリーを実行する方法を示します。また、ポートに接続しているデバイスを確認するためのクエリーの実行対象ポートから受信した応答が IEEE 802.1X 対応であることを示します。

```
Device> enable
Device# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

Related Commands	コマンド	説明
	dot1x test timeout <i>timeout</i>	IEEE 802.1X 準備クエリーに されるタイムアウトを設定

dot1x test timeout

IEEE 802.1X 準備状態を照会しているポートからの EAPOL 応答の待機に使用されるタイムアウトを設定するには、グローバル コンフィギュレーション モードで **dot1x test timeout** コマンドを使用します。

dot1x test timeout *timeout*

Syntax Description	<i>timeout</i>	EAPOL 応答を待機する時間（秒）。指定できる範囲は 1 ～ 65535 秒です。
---------------------------	----------------	--

Command Default	デフォルト設定は 10 秒です。
------------------------	------------------

Command Modes	グローバル コンフィギュレーション（config）
----------------------	---------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines	EAPOL 応答を待機するために使用されるタイムアウトを設定するには、このコマンドを使用します。
-------------------------	--

このコマンドには、no 形式はありません。

次の例では、EAPOL 応答を 27 秒間待機するようにスイッチを設定する方法を示します。

```
Device> enable
Device# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show running-config** コマンドを入力します。

Related Commands	コマンド	説明
	dot1x test eapol-capable [interface interface-id]	すべての、または指定された IEEE 802.1X 対応ポートに接続するデバイスで IEEE 802.1X の準備が整っているかを確認します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバルコンフィギュレーションモードまたはインターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。再試行タイムアウトをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout { **auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

Syntax Description

auth-period *seconds*

サブリカントで保留ステートが維持される秒数（つまり、サブリカントが試行に失敗した場合に再度クレデンシアルを送信するまでに待機する時間）を設定します。

有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。

held-period *seconds*

サブリカントで保留ステートが維持される秒数（つまり、サブリカントが試行に失敗した場合に再度クレデンシアルを送信するまでに待機する時間）を設定します。

有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。

quiet-period *seconds*

認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケーター（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。

有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。

ratelimit-period *seconds*

動作の不正なクライアント PC（たとえば、デバイス処理電力の無駄につながる、EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。

- オーセンティケーターはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。
- 有効な範囲は 1 ～ 65535 です。デフォルトでは、レート制限はディセーブルになっています。

server-timeout *seconds*

連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。

- 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。

サーバが指定時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。

start-period <i>seconds</i>	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
supp-timeout <i>seconds</i>	EAP 要求 ID 以外のすべての EAP メッセージについて、オーセンティケータからホストへの再送信時間を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
tx-period <i>seconds</i>	クライアントに EAP 要求 ID パケットを再送信する間隔を（応答が受信されないものと仮定して）秒数で設定します。 <ul style="list-style-type: none"> 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 802.1X パケットがサブリカントに送信され、そのサブリカントが再試行期間後に応答しなかった場合、そのパケットは再度送信されます。

Command Default 定期的な再認証と定期的なレート制限が行われます。

Command Modes グローバル コンフィギュレーション (config)
インターフェイス コンフィギュレーション (config-if)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

dot1x reauthentication インターフェイス コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにした場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、デバイスの動作に影響します。

待機時間の間、デバイスはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい数を入力することによって、ユーザへの応答時間を短縮できます。

ratelimit-period が 0（デフォルト）に設定された場合、デバイスは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバに転送します。

次に、さまざまな 802.1X 再送信およびタイムアウト時間が設定されている例を示します。

```
Device> enable
Device(config)# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
```

```
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
Device(config-if)# end
```

dtls

Datagram Transport Layer Security (DTLS) のパラメータを設定するには、RADIUS サーバコンフィギュレーションモードで **dtls** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dtls

connectiontimeout *connection-timeout-value* | **idletimeout** *idle-timeout-value* [| **ip** | **ipv6**] { **radius source-interface** *interface-name* | **vrf forwarding** *forwarding-table-name* } | **match-server-identity** { **email-address** *email-address* | **hostname** *hostname* | **ip-address** *ip-address* } | **port** *port-number* | **retries** *number-of-connection-retries* | **trustpoint** { **client** *trustpoint name* | **server** *trustpoint name* }

no dtls

Syntax Description

connectiontimeout <i>connection-timeout-value</i>	(任意) DTLS 接続タイムアウト値を設定します。
idletimeout <i>idle-timeout-value</i>	(任意) DTLS アイドルタイムアウト値を設定します。
[ip ipv6] { radius source-interface <i>interface-name</i> vrf forwarding <i>forwarding-table-name</i> }	(任意) IP または IPv6 送信元パラメータを設定します。
match-server-identity { email-address <i>email-address</i> hostname <i>host-name</i> ip-address <i>ip-address</i> }	RadSec 認定検証パラメータを設定します。
port <i>port-number</i>	(任意) DTLS ポート番号を設定します。
retries <i>number-of-connection-retries</i>	(任意) DTLS 接続再試行の回数を設定します。
trustpoint { client <i>trustpoint name</i> server <i>trustpoint name</i> }	(任意) クライアントとサーバに DTLS トラストポイントを設定します。

Command Default

- DTLS 接続タイムアウトのデフォルト値は 5 秒です。
- DTLS アイドルタイムアウトのデフォルト値は 60 秒です。
- デフォルトの DTLS ポート番号は 2083 です。
- DTLS 接続再試行回数のデフォルト値は 5 です。

Command Modes

RADIUS サーバ コンフィギュレーション (config-radius-server)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	match-server-identity キーワードが導入されました。
Cisco IOS XE Amsterdam 17.1.1	ipv6 キーワードが導入されました。

Usage Guidelines

認証、許可、およびアカウントティング（AAA）サーバグループでは、すべてで同じサーバタイプを使用し、Transport Layer Security（TLS）のみか DTLS のみにすることを推奨します。

Examples

次に、DTLS 接続タイムアウト値を 10 秒に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# dtls connectiontimeout 10
Device(config-radius-server)# end
```

Related Commands

Command	Description
show aaa servers	DTLS サーバに関連する情報を表示します。
clear aaa counters servers radius {server id all}	RADIUS DTLS 固有の統計情報をクリアします。
debug radius dtls	RADIUS DTLS 固有のデバッグを有効にします。

enable password

さまざまな権限レベルへのアクセスを制御するローカルパスワードを設定するには、グローバルコンフィギュレーションモードで **enable password** コマンドを使用します。ローカルパスワードの制御アクセスを削除するには、このコマンドの **no** 形式を使用します。

enable password [level *level*] {[0] *unencrypted-password* | [*encryption-type*] *encrypted-password*}
no enable password [level *level*]

Syntax Description

level *level*

(任意) パスワードが適用されるレベルを指定します。0～15の数字を使用して権限レベルを指定できます。レベル1が通常のユーザ EXEC モードユーザコマンドまたはコマンドの **no** 形式で指定されていない場合、権限レベルは1になります。

0

(任意) 暗号化されていないクリアテキストパスワードを指定します。パスワードハッシュアルゴリズム (SHA) 256 シークレットに変換されてデバイス

unencrypted-password

イネーブルモードを開始するためのパスワードを指定します。

encryption-type

(任意) パスワードの暗号化に使用するシスコ独自のアルゴリズム。暗号化する場合、入力する次の引数は暗号化されたパスワード (すでにシスコで暗号化されたパスワード) である必要があります。非表示のパスワードが続く場合は、7を指定できます。

encrypted-password

別のデバイス設定からコピーした暗号化パスワード。

Command Default

パスワードは定義されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが追加された。

Usage Guidelines

enable password コマンドと **enable secret** コマンドのいずれも設定されていない場合、コンソールの回線パスワードが設定されていれば、コンソールの回線パスワードがすべての VTY (Telnet およびセキュアシェル (SSH)) セッションのイネーブルパスワードとして機能します。

特定の権限レベルのパスワードを定義する場合は、**level** オプションを指定して **enable password** コマンドを使用します。レベルとパスワードを設定したら、このレベルにアクセスする必要があるユーザとパスワードを共有します。各レベルでアクセスできるコマンドを指定するには、**privilege level** コンフィギュレーション コマンドを使用します。

通常、暗号化タイプは、シスコデバイスによってすでに暗号化されているパスワードをコピーしてこのコマンドに貼り付ける場合にのみ入力します。



Caution 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。以前に暗号化されたパスワードを忘れた場合、回復することはできません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを実行すると、**enable password** コマンドで作成するパスワードが暗号化された形式で表示されます。

service password-encryption コマンドを使用して、パスワードの暗号化を有効または無効にすることができます。

イネーブルパスワードの定義は次のとおりです。

- 数字、大文字、小文字を組み合わせた 1 ～ 25 文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、**Ctrl+V** キーの組み合わせを押してから疑問符 (?) を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。
 1. **abc** を入力します。
 2. **Ctrl-v** を押します。
 3. **?123** を入力します。



Note システムから **enable password** コマンドを入力するように求められた場合、疑問符の前に **Ctrl+V** を入力する必要はなく、パスワードのプロンプトにそのまま *abc?123* と入力できます。

Examples

次に、特権レベル 2 のパスワード `pswd2` を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 pswd2
```

次に、暗号化タイプ 7 を使用して、デバイスのコンフィギュレーションファイルからコピーした権限レベル 2 の暗号化パスワード `1i5Rkls3LoyxzS8t9` を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
enable secret	enable password コマンドよりも強化したセキュリティです。
service password-encryption	パスワードを暗号化します。
more nvram:startup-config	NVRAMに保管されている、またはCONFIG_FILE環境されているスタートアップ コンフィギュレーションを表示します。
privilege level	ユーザの権限レベルを設定します。

enable secret

enable password コマンドよりも強化したセキュリティレイヤを指定するには、グローバル コンフィギュレーション モードで **enable secret** コマンドを使用します。イネーブルシークレット機能をオフにするには、このコマンドの **no** 形式を使用します。

enable secret [*level level*] {[**0**] *unencrypted-password* | *encryption-type encrypted-password*}

no enable secret [*level level*] [*encryption-type encrypted-password*]

Syntax Description

level level

(任意) パスワードが適用されるレベルを指定します。1 ~ 15 の数字を権限レベルを指定できます。レベル 1 が通常のユーザ EXEC モード権限。コマンドまたはコマンドの **no** 形式で指定されていない場合、権限レベルはデフォルトです。

0

(任意) 暗号化されていないクリアテキストパスワードを指定します。パスワードは SHA-256 ハッシュ アルゴリズム (SHA) 256 シークレットに変換されてデバイスに保存されます。

unencrypted-password

ユーザがイネーブルモードを開始するためのパスワードを指定します。**enable password** コマンドで作成したパスワードとは異なるものにすることを強制します。

encryption-type

パスワードのハッシュに使用するシスコ独自のアルゴリズム。

- **5:** メッセージダイジェストアルゴリズム 5 (MD5) で暗号化されたパスワードを指定します。
- **8:** パスワードベースキー派生関数 2 (PBKDF2) の SHA-256 でハッシュされたパスワードを指定します。
- **9:** スクリプトでハッシュされたシークレットを指定します。

encrypted-password

別のデバイス設定からコピーしたハッシュパスワード。

Command Default

パスワードは定義されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入された。

Usage Guidelines

enable password コマンドと **enable secret** コマンドのいずれも設定されていない場合、コンソールの回線パスワードが設定されていれば、コンソールの回線パスワードがすべての VTY (Telnet およびセキュアシェル (SSH)) セッションのイネーブルパスワードとして機能します。

enable secret コマンドは、**enable password** パスワードよりも強化したセキュリティレイヤを指定するために使用します。**enable secret** コマンドでは、不可逆的な暗号化機能を使用してパスワードを保存することでセキュリティを向上させます。この追加のセキュリティ暗号化レイヤは、パスワードがネットワークで送信される環境や TFTP サーバに保存される環境において役立ちます。

通常、暗号化タイプは、デバイスのコンフィギュレーションファイルからコピーした暗号化パスワードをこのコマンドに貼り付ける場合にのみ入力します。



Caution 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。以前に暗号化されたパスワードを忘れた場合、回復することはできません。

enable password コマンドと **enable secret** コマンドに同じパスワードを使用した場合、推奨されない方法であることを警告するエラーメッセージが表示されますが、パスワードは受け入れられます。ただし、同じパスワードを使用すると、**enable secret** コマンドによって提供される追加のセキュリティが損なわれます。



Note **enable secret** コマンドを使用してパスワードを設定した後、**enable password** コマンドを使用して設定したパスワードは、**enable secret** が無効になっている場合にのみ機能します。また、いずれの方法で暗号化したパスワードも、忘れた場合は回復できません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを実行すると、作成するパスワードが暗号化された形式で表示されます。

service password-encryption コマンドを使用して、パスワードの暗号化を有効または無効にすることができます。

イネーブルパスワードの定義は次のとおりです。

- 数字、大文字、小文字を組み合わせた 1 ~ 25 文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、**Crtl+V** キーの組み合わせを押してから疑問符 (?) を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。

1. **abc** を入力します。
2. **Crtl-v** を押します。
3. **?123** を入力します。



Note システムから **enable password** コマンドを入力するように求められた場合、疑問符の前に Ctrl+V を入力する必要はなく、パスワードのプロンプトにそのまま **abc?123** と入力できます。

Examples

次に、**enable secret** コマンドを使用してパスワードを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

enable secret コマンドを使用してパスワードを指定した後、ユーザはこのパスワードを入力してアクセスする必要があります。**enable password** コマンドを使用して設定されたパスワードは機能しなくなります。

```
Password: password
```

次に、暗号化タイプ 4 を使用して、デバイスのコンフィギュレーション ファイルからコピーした権限レベル 2 の暗号化パスワード **\$1\$FaD0\$Xyti5Rkls3LoyxzS8** を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

次に、ユーザが **enable secret 4 encrypted-password** コマンドを入力したときに表示される警告メッセージの例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

WARNING: Command has been added to the configuration but Type 4 passwords have been deprecated.
Migrate to a supported password type

Device(config)# end
Device# show running-config | inc secret

enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

Related Commands

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するロ設定します。

コマンド	説明
more nvram:startup-config	NVRAMに保管されている、またはCONFIG_FILE環境設定されているスタートアップ コンフィギュレーションを読み込みます。
service password-encryption	パスワードを暗号化します。

epm access-control open

アクセスコントロールリスト（ACL）が設定されていないポートにオープンディレクティブを設定するには、グローバルコンフィギュレーションモードで **epm access-control open** コマンドを使用します。オープンディレクティブをディセーブルにするには、このコマンドの **no** 形式を使用します。

epm access-control open
no epm access-control open

Syntax Description

このコマンドには、引数またはキーワードはありません。

Command Default

デフォルトのディレクティブが適用されます。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スタティック ACL が設定されたアクセスポートに、認可ポリシーのないホストを許可するオープンディレクティブを設定するには、このコマンドを使用します。このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープンの両方のディレクティブがポートへのアクセスを許可します。

設定を確認するには、**show running-config** コマンドを入力します。

次の例では、オープンディレクティブを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# epm access-control open
Device(config)# exit
```

Related Commands

コマンド	説明
show running-config	現在実行されているコンフィギュレーションファイルの内容を表示します

include-icv-indicator

MKPDUに整合性チェック値（ICV）インジケータを含めるには、MKA ポリシー コンフィギュレーションモードで **include-icv-indicator** コマンドを使用します。ICVインジケータを無効にするには、このコマンドの **no** 形式を使用します。

include-icv-indicator
no include-icv-indicator

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default ICV インジケータが含まれています。

Command Modes MKA ポリシー コンフィギュレーション（config-mka-policy）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、MKPDUにICVインジケータを含める例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# include-icv-indicator
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

ip access-list

IP アクセスリストまたはオブジェクトグループ アクセス コントロール リスト (ACL) を名前または番号によって定義する場合、または、IP ヘルパーアドレス宛先をもつパケットのフィルタリングを有効にする場合は、グローバル コンフィギュレーション モードで **ip access-list** コマンドを使用します。IP アクセスリストまたはオブジェクトグループ ACL を削除する場合、または、IP ヘルパーアドレス宛先をもつパケットのフィルタリングを無効にする場合は、このコマンドの **no** 形式を使用します。

```
ip access-list { {extended | resequence | standard} {access-list-numberaccess-list-name} | helper egress check | log-update threshold threshold-number | logging {hash-generation | interval time} | persistent | role-based access-list-name}
```

```
ip access-list { {extended | resequence | standard} {access-list-numberaccess-list-name} | helper egress check | log-update threshold | logging {hash-generation | interval} | persistent | role-based access-list-name}
```

Syntax Description	
standard	標準 IP アクセスリストを指定します。
resequence	並べ直した IP アクセスリストを指定します。
extended	拡張 IP アクセスリストを指定します。オブジェクトグループ ACL の場合は必須です。
<i>access-list-name</i>	IP アクセスリストまたはオブジェクトグループ ACL の名前。この名前にはスペースまたは引用符を含めることはできず、番号付けされたアクセスリストと紛らわしくならないよう、英文字で始める必要があります。
<i>access-list-number</i>	アクセスリストの番号。 <ul style="list-style-type: none"> 標準 IP アクセスリストの範囲は 1 ～ 99 または 1300 ～ 1999 です。 拡張 IP アクセスリストの範囲は 100 ～ 199 または 2000 ～ 2699 です。
helper egress check	IP ヘルパー機能を介して宛先サーバアドレスにリレーされるトラフィックについて、インターフェイスに適用される発信アクセスリストの許可または拒否の照合機能を有効にします。
log-update	アクセスリストログの更新を制御します。
threshold <i>threshold-number</i>	アクセスリストログのしきい値を設定します。指定できる範囲は 0 ～ 2147483647 です。
logging	アクセスリストのロギングを制御します。
hash-generation	syslog ハッシュコードの生成を有効にします。

interval time	アクセスリストのロギング間隔をミリ秒単位で設定します。指定できる範囲は 0 ～ 2147483647 です。
persistent	アクセスコントロールエントリ（ACE）のシーケンス番号は、リロード後も保持されます。 Note これはデフォルトで有効であり、無効にすることはできません。
role-based	ロールベースの IP アクセスリストを指定します。

Command Default

IP アクセスリストまたはオブジェクトグループ ACL が定義されていないため、発信 ACL は IP ヘルパーによってリレーされたトラフィックを照合およびフィルタリングしません。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

名前付きまたは番号付き IP アクセスリストまたはオブジェクトグループ ACL を設定するには、このコマンドを使用します。コマンドによって、デバイスはアクセスリスト コンフィギュレーション モードを開始します。ここで、**deny** コマンドおよび **permit** コマンドを使用して、拒否アクセス条件または許可アクセス条件を定義しなければなりません。

ip access-list コマンドで **standard** または **extended** のキーワードを指定することで、アクセスリスト コンフィギュレーションモードを開始したときに表示されるプロンプトが決定されます。オブジェクトグループ ACL を定義する場合は、**extended** キーワードを使用する必要があります。

オブジェクトグループと IP アクセスリスト、またはオブジェクトグループ ACL を個別に作成できます。つまり、まだ存在しないオブジェクトグループ名を使用できます。

ip access-group コマンドを使用して、アクセスリストをインターフェイスに適用します。

ip access-list helper egress check コマンドは、IP ヘルパーアドレス宛先をもつパケットの許可または拒否機能の発信 ACL マッチングを有効にします。このコマンドで発信拡張 ACL を使用すると、送信元または宛先の User Datagram Protocol（UDP）ポートに基づいて、IP ヘルパーリレートラフィックを許可または拒否できます。**ip access-list helper egress check** コマンドはデフォルトでは無効です。発信 ACL は、IP ヘルパーによってリレーされたトラフィックを照合およびフィルタリングしません。

Examples

次に、Internetfilter という名前の標準アクセスリストを定義する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard Internetfilter
Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255
```

```
Device(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Device(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

次に、プロトコルポートが `my_service_object_group` で指定されたポートと一致する場合に、`my_network_object_group` 内のユーザからのパケットを許可するオブジェクトグループ ACL を作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended my_ogacl_policy
Device(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any
Device(config-ext-nacl)# deny tcp any any
```

次に、ヘルパーアドレスの宛先をもつパケットで発信 ACL フィルタリングを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list helper egress check
```

Related Commands

Command	Description
deny	パケットを拒否する名前付き IP アクセスリストまたはオブジェクトグループ ACL の条件を設定します。
ip access-group	ACL またはオブジェクトグループ ACL をインターフェイスまたはサービスポリシーマップに適用します。
object-group network	オブジェクトグループ ACL で使用するネットワーク オブジェクトグループを定義します。
object-group service	オブジェクトグループ ACL で使用するサービス オブジェクトグループを定義します。
permit	パケットを許可する名前付き IP アクセスリストまたはオブジェクトグループ ACL の条件を設定します。
show ip access-list	IP アクセスリストまたはオブジェクトグループ ACL の内容を表示します。
show object-group	設定されているオブジェクトグループに関する情報を表示します。

ip access-list role-based

ロールベース（セキュリティグループ）アクセスコントロールリスト（RBACL）を作成して、ロールベース ACL コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **ip access-list role-based** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

```
ip access-list role-based access-list-name
no ip access-list role-based access-list-name
```

Syntax Description

access-list-name セキュリティグループアクセスコントロールリスト（SGACL）の名前。

Command Default

ロールベースの ACL は設定されていません。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

SGACL ロギングの場合は、**permit ip log** コマンドを設定する必要があります。また、このコマンドは、ダイナミック SGACL のロギングを有効にするために、Cisco Identity Services Engine（ISE）でも設定する必要があります。

次に、IPv4トラフィックに適用できる SGACL を定義し、ロールベース アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list role-based rbacl1
Device(config-rb-acl)# permit ip log
Device(config-rb-acl)# end
```

Related Commands

コマンド	説明
permit ip log	設定されたエントリに一致するロギングを許可します。
show ip access-list	現在のすべての IP アクセスリストの内容を表示します。

ip admission

Web 認証を有効にするには、インターフェイス コンフィギュレーション モードまたはフォールバックプロファイル コンフィギュレーション モードで **ip admission** コマンドを使用します。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip admission rule
no ip admission rule

Syntax Description	<i>rule</i> IP アドミッションルールの名前。				
Command Default	Web 認証はディセーブルです。				
Command Modes	インターフェイス コンフィギュレーション (config-if) フォールバックプロファイル コンフィギュレーション (config-fallback-profile)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines **ip admission** コマンドはスイッチポートに web 認証ルールを適用します。

次の例では、スイッチポートに Web 認証ルールを適用する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
Device(config-if)# end
```

次の例では、IEEE 802.1X 対応のスイッチポートで使用するフォールバックプロファイルに Web 認証ルールを適用する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
Device(config-fallback-profile)# end
```

ip admission name

Web 認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ip admission name** コマンドを使用します。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time
minutes | list {acl | acl-name} | service-policy type tag service-policy-name]
no ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time
minutes | list {acl | acl-name} | service-policy type tag service-policy-name]
```

Syntax Description

name	ネットワークアドミッション制御ルールの名前。
consent	認証プロキシ同意 Web ページを <i>admission-name</i> 引数で指定された IP アドミッションルールに対応させます。
proxy http	Web 認証のカスタムページを設定します。
absolute-timer 分	(任意) 外部サーバがタイムアウトするまでの経過時間 (分)。
inactivity-time 分	(任意) 外部ファイルサーバが到達不能であると見なされるまでの経過時間 (分)。
list	(任意) 指定されたルールをアクセスコントロールリスト (ACL) に関連付けます。
acl	標準、拡張リストを指定のアドミッション制御ルールに適用します。値の範囲は 1~199、または拡張範囲で 1300 から 2699 です。
acl-name	名前付きのアクセスリストを指定のアドミッション制御ルールに適用します。
service-policy type tag	(任意) コントロールプレーン サービス ポリシーを設定できます。
service-policy-name	policy-map type control tag <i>polycyname</i> コマンド、キーワード、および引数を使用して設定されたコントロールプレーンタグのサービスポリシー。このポリシーマップは、タグを受信したときのホストでの処理を適用するために使用されます。

Command Default

Web 認証はディセーブルです。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

ip admission name コマンドにより、スイッチ上で Web 認証がグローバルにイネーブルになります。

スイッチ上で Web 認証をイネーブルにしてから、**ip access-group in** および **ip admission web-rule** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイス上で Web 認証をイネーブルにします。

Examples

次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
Device(config-if)# end
```

次の例では、スイッチ ポートでのフォールバックメカニズムとして、Web 認証とともに IEEE 802.1X 認証を設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

Related Commands

コマンド	説明
dot1x fallback	IEEE 802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	Web 認証のフォールバックプロファイルを作成します。
ip admission	ポートで Web 認証をイネーブルにします。

コマンド	説明
show authentication sessions interface <i>interface</i> detail	Web 認証セッションのステータスに関する情報を表示します。
show ip admission	NAC のキャッシュされたエントリまたは NAC 設定についての情報を表示します。

ip dhcp snooping database

Dynamic Host Configuration Protocol (DHCP) のスヌーピングデータベースを設定するには、グローバル コンフィギュレーション モードで **ip dhcp snooping database** コマンドを使用します。DHCP スヌーピングサーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip dhcp snooping database { crashinfo: url | flash: url | ftp: url | http: url | https: url
| rcp: url | scp: url | tftp: url | timeout seconds | usbflash0: url | write-delay
seconds }
no ip dhcp snooping database [ timeout | write-delay ]
abon
```

Syntax Description

crashinfo: url	crashinfo を使用して、エントリーを格納するためのデータベースの URL を指定します。
flash: url	flash を使用して、エントリーを格納するためのデータベースの URL を指定します。
ftp: url	FTP を使用して、エントリーを格納するためのデータベースの URL を指定します。
http: url	HTTP を使用して、エントリーを格納するためのデータベースの URL を指定します。
https: url	セキュア HTTP (HTTPS) を使用して、エントリーを格納するためのデータベースの URL を指定します。
rcp: url	リモートコピー (RCP) を使用して、エントリーを格納するためのデータベースの URL を指定します。
scp: url	セキュアコピー (SCP) を使用して、エントリーを格納するためのデータベースの URL を指定します。
tftp: url	TFTP を使用して、エントリーを格納するためのデータベースの URL を指定します。

timeout <i>seconds</i>	キャンセルタイムアウトインターバルを指定します。有効値は 0 ~ 86,400 秒です。
usbflash0:url	USB flash を使用して、エントリーを格納するためのデータベースの URL を指定します。
write-delay <i>seconds</i>	ローカル DHCP スヌーピングデータベースにデータが追加されてから、DHCP スヌーピングエントリーを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ~ 86,400 秒です。

Command Default DHCP スヌーピングデータベースは設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを入力する前に、インターフェイス上で DHCP スヌーピングをイネーブルにする必要があります。DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
Device(config)# exit
```

次に、DHCP スヌーピングエントリーを外部サーバに書き込むまでの時間を指定する例を示します。

```
evice> enable
Device# configure terminal
Device(config)# ip dhcp snooping database write-delay 15
Device(config)# exit
```

ip dhcp snooping information option format remote-id

オプション 82 リモート ID サブオプションを設定するには、デバイスのグローバル コンフィギュレーションモードで **ip dhcp snooping information option format remote-id** コマンドを使用します。デフォルトのリモート ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

```
ip dhcp snooping information option format remote-id {hostname | string string}
no ip dhcp snooping information option format remote-id {hostname | string string}
```

Syntax Description

hostname デバイスのホスト名をリモート ID として指定します。

string string 1～63 の ASCII 文字（スペースなし）を使用して、リモート ID を指定します。

Command Default

デバイスの MAC アドレスは、リモート ID です。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

Usage Guidelines

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用して DHCP スヌーピングをグローバルにイネーブルにする必要があります。

オプション 82 機能がイネーブルの場合、デフォルトのリモート ID サブオプションはデバイスの MAC アドレスです。このコマンドを使用すると、デバイスのホスト名または 63 個の ASCII 文字列（スペースなし）のいずれかをリモート ID として設定できます。



Note ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。

次の例では、オプション 82 リモート ID サブオプションを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping information option format remote-id hostname
Device(config)# exit
```

ip dhcp snooping verify no-relay-agent-address

DHCP クライアントメッセージのリレーエージェントアドレス (giaddr) が信頼できないポート上のクライアントハードウェアアドレスに一致することを確認して、DHCP スヌーピング機能をディセーブルにするには、グローバルコンフィギュレーションモードで **ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証をイネーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address

Syntax Description	このコマンドには引数またはキーワードはありません。	
Command Default	DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアントメッセージのリレーエージェント IP アドレス (giaddr) フィールドが 0 であることを確認します。	
Command Modes	グローバルコンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	<p>デフォルトでは、DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアントメッセージのリレーエージェントの IP アドレス (giaddr) フィールドが 0 であることを確認します。giaddr フィールドが 0 でない場合、メッセージはドロップされます。検証をディセーブルにするには、ip dhcp snooping verify no-relay-agent-address コマンドを使用します。検証を再度イネーブルにするには、no ip dhcp snooping verify no-relay-agent-address コマンドを使用します。</p> <p>次に、DHCP クライアントメッセージの giaddr 検証をイネーブルにする例を示します。</p> <pre>Device> enable Device# configure terminal Device(config)# no ip dhcp snooping verify no-relay-agent-address Device(config)# exit</pre>	

ip http access-class

HTTP サーバへのアクセスを制限するために使用するアクセスリストを指定するには、グローバル コンフィギュレーション モードで **ip http access-class** コマンドを使用します。以前に設定したアクセスリストの関連付けを削除するには、このコマンドの **no** 形式を使用します。

```
ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name } |
ipv6 access-list-name }
no ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name }
| ipv6 access-list-name }
```

Syntax Description

<i>access-list-number</i>	グローバル コンフィギュレーション コマンド access-list を使用して設定される、0 ~ 99 の標準 IP アクセスリスト番号。
ipv4	セキュア HTTP サーバへのアクセスを制限するように IPv4 アクセス リストを指定します。
<i>access-list-name</i>	ip access-list コマンドで設定された標準 IPv4 アクセスリストの名前。
ipv6	セキュア HTTP サーバへのアクセスを制限するように IPv6 アクセス リストを指定します。

Command Default

アクセス リストは、HTTP サーバには適用されません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドが設定されていると、指定されたアクセス リストは HTTP サーバに割り当てられません。HTTP サーバは、接続を受け入れる前にアクセス リストを確認します。確認に失敗すると、HTTP サーバは接続要求を承認しません。

Examples

次に、アクセス リストを 20 に定義して、HTTP サーバに割り当てる例を示します。

```
Device> enable
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
Device(config)# ip http access-class 20
Device(config-std-nacl)# exit
```

次に、IPv4 の指定済みアクセス リストを定義して、HTTP サーバに割り当てる例を示します。

```
Device> enable
Device(config)# ip access-list standard Internet_filter
Device(config-std-nacl)# permit 1.2.3.4
Device(config-std-nacl)# exit
Device(config)# ip http access-class ipv4 Internet_filter
Device(config)# exit
```

Related Commands

コマンド	説明
ip access-list	ID をアクセス リストに割り当て、アクセス リストのコンフィギュレーション モードを開始します。
ip http server	HTTP 1.1 サーバ（Cisco Web ブラウザ ユーザ インターフェイスを含む）をイネーブルにします。

ip radius source-interface

すべての発信 RADIUS パケットに対して指定されたインターフェイスの IP アドレスを使用するように RADIUS を設定するには、グローバル コンフィギュレーション モードで **ip radius source-interface** コマンドを使用します。すべての発信 RADIUS パケットに対して指定されたインターフェイスの IP アドレスを使用しないように RADIUS を設定するには、このコマンドの **no** 形式を使用します。

ip radius source-interface *interface-name* [**vrf** *vrf-name*]
no ip radius source-interface

Syntax Description	
<i>interface-name</i>	RADIUS がすべての発信パケットに使用するインターフェイスの名前です。
vrf <i>vrf-name</i>	(任意) Virtual Route Forwarding (VRF) 単位の設定です。

Command Default デフォルトの動作や値はありません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、すべての発信 RADIUS パケットの送信元アドレスとして使用するインターフェイスの IP アドレスを設定する場合に使用します。インターフェイスがアップ状態である限り、この IP アドレスが使用されます。RADIUS サーバでは、IP アドレスのリストを保持する代わりに、すべてのネットワーク アクセス クライアントに対して 1 つの IP アドレスエントリを使用できます。インターフェイスがアップ状態であるかダウン状態であるかに関係なく、関連付けられているインターフェイスの IP アドレスが使用されます。

特に、ルータに多数のインターフェイスがあり、特定のルータからのすべての RADIUS パケットに同一の IP アドレスが含まれるようにする場合は、**ip radius source-interface** コマンドが役立ちます。

指定されたインターフェイスに有効な IP アドレスがあり、アップ状態でないと、設定は有効になりません。指定されたインターフェイスに有効な IP アドレスがない場合やダウン状態である場合、RADIUS によって AAA サーバへの最適なルートに対応するローカル IP が選択されます。これを回避するには、インターフェイスに有効な IP アドレスを追加するか、そのインターフェイスをアップ状態にします。

このコマンドを VRF 単位で設定するには、**vrf vrf-name** キーワードと引数を使用します。これにより、ユーザのルートに別のユーザのルートとの相互関係がない複数のルーティングテーブルまたは転送テーブルを使用できます。

Examples

次に、すべての発信 RADIUS パケットに対してインターフェイス s2 の IP アドレスを使用するように RADIUS を設定する例を示します。

```
ip radius source-interface s2
```

次に、VRF の定義に対してインターフェイス Ethernet0 の IP アドレスを使用するように RADIUS を設定する例を示します。

```
ip radius source-interface Ethernet0 vrf vrf1
```

ip source binding

スタティック IP ソース バインディング エントリを追加するには、**ip source binding** コマンドを使用します。スタティック IP ソース バインディング エントリを削除するには、このコマンドの **no** 形式を使用します。

```
ip source binding mac-address vlan vlan-id ip-address interface interface-id
no ip source binding mac-address vlan vlan-id ip-address interface interface-id
```

Syntax Description		
<i>mac-address</i>		バインディング対象 MAC アドレスです。
vlan <i>vlan-id</i>		レイヤ 2 VLAN ID を指定します。有効な値は 1~4094 です。
<i>ip-address</i>		バインディング対象 IP アドレスです。
interface <i>interface-id</i>		物理インターフェイスの ID です。

Command Default IP 送信元バインディングは設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History		変更内容
リリース		
Cisco IOS XE Fuji 16.9.2		このコマンドが導入されました。

Usage Guidelines このコマンドは、スタティック IP ソース バインディング エントリだけを追加するために使用できます。

no 形式は、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。コマンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディング エントリが新しいパラメータで更新されます。

次の例では、スタティック IP ソース バインディング エントリを追加する方法を示します。

```
Device> enable
Device# configure terminal
Device(config) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
Device(config)# exit
```

ip ssh source-interface

インターフェイスの IP アドレスをセキュアシェル（SSH）クライアントデバイスの送信元アドレスとして指定するには、グローバルコンフィギュレーションモードで **ip ssh source-interface** コマンドを使用します。送信元アドレスとして指定した IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
ip ssh source-interface interface
no ip ssh source-interface interface
```

Syntax Description

<i>interface</i>	アドレスを SSH クライアントの送信元アドレスとして使用するインターフェイス。
------------------	--

Command Default

宛先に最も近いインターフェイスのアドレスが送信元アドレスとして使用されます（最も近いインターフェイスは SSH パケットが送信される出力インターフェイスです）。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	

Usage Guidelines

このコマンドを指定することにより、SSH クライアントの送信元アドレスとして送信元インターフェイスの IP アドレスを使用するように強制できます。

Examples

次の例では、GigabitEthernet インターフェイス 1/0/1 に割り当てられた IP アドレスが SSH クライアントの送信元アドレスとして使用されます。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh source-interface GigabitEthernet 1/0/1
Device(config)# exit
```

ip verify source

インターフェイス上の IP ソース ガードを有効にするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガードを無効にするには、このコマンドの **no** 形式を使用します。

ip verify source [mac-check][tracking]
no ip verify source

mac-check	(任意) MAC アドレス検証による IP ソース ガードをイネーブルにします。
tracking	(任意) ポートで静的 IP アドレス を学習するために IP ポート セキュリティをイネーブルにします。

Command Default IP 送信元ガードはディセーブルです。

Command Modes インターフェイス コンフィギュレーション (config-if)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

送信元 IP アドレス フィルタリングおよび MAC アドレス検証による IP ソース ガードをイネーブルにするには、**ip verify source mac-check** インターフェイス コンフィギュレーション コマンドを使用します。

Examples

次の例では、送信元 IP アドレス フィルタリングによる IP ソース ガードをインターフェイス上でイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
Device(config-if)# end
```

次の例では、MAC アドレスの検証による IP ソース ガードをイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check
```

```
Device(config-if)# end
```

設定を確認するには、**show ip verify source** コマンドを入力します。

ipv6 access-list

IPv6 アクセス リストを定義してデバイスを IPv6 アクセス リスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*
noipv6 access-list *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

Syntax Description	
ipv6 <i>access-list-name</i>	名前付き IPv6 ACL（最長 64 文字）を作成し、IPv6 ACL コンフィギュレーション モードを開始します。 <i>access-list-name</i> : IPv6 アクセスリストの名前。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
match-local-traffic	ローカルで生成されたトラフィックに対する照合を有効にします。
log-update threshold <i>threshold-in-msgs</i>	最初のパケットの一致後に、syslog メッセージを生成する方法を決定します。 <i>threshold-in-msgs</i> : 生成されるパケット数。
role-based <i>list-name</i>	ロールベースの IPv6 ACL を作成します。

Command Default IPv6 アクセス リストは定義されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	
リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することで定義され、その許可と拒否の条件は IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用することで設定されます。 **ipv6 access-list** コマンドを設定すると、デバイスは IPv6 アクセス リスト コンフィギュレーション モードになります。 IPv6 アクセス リスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。



Note IPv6 ACL は一意な名前によって定義されます (IPv6 は番号付けされた ACL をサポートしません)。 IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** ステートメントおよび **deny any any** ステートメントでプロトコル タイプとして自動的に設定されます。

IPv6 ACL にはそれぞれ、最後に一致した条件として、暗黙の **permit icmp any any nd-na** ステートメント、**permit icmp any any nd-ns** ステートメント、および **deny ipv6 any any** ステートメントがあります（前の2つの一致条件は、ICMPv6 ネイバー探索を許可します）。1つの IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも1つのエントリが含まれている必要があります。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

IPv6 ACL を IPv6 インターフェイスに適用するには、*access-list-name* 引数を指定して **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ACL をデバイスとの着信および発信 IPv6 仮想端末接続に適用するには、*access-list-name* 引数を指定して、**ipv6 access-class** ライン コンフィギュレーション コマンドを使用します。

ipv6 traffic-filter コマンドでインターフェイスに適用される IPv6 ACL は、デバイスによって発信されたトラフィックではなく、転送されたトラフィックをフィルタ処理します。

Examples

次に、list1 という名前の IPv6 ACL を設定し、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)# end
```

次に、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用する例を示します。特に、最初の ACL エントリは、ネットワーク FEC0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカルプレフィックス FEC0:0:0:2 を持つパケット）が GigabitEthernet インターフェイス 0/1/2 から出て行くことを拒否します。2 番目の ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。2 番目のエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# ipv6 traffic-filter list2 out
Device(config-if)# end
```

ipv6 snooping policy

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 snooping policy** コマンドを使用します。IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

Syntax Description	<i>snooping-policy</i> スヌーピング ポリシーのユーザ定義名。ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。				
Command Default	IPv6 スヌーピング ポリシーは設定されていません。				
Command Modes	グローバル コンフィギュレーション（config）				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines IPv6 スヌーピング ポリシーを作成するには、**ipv6 snooping policy** コマンドを使用します。**ipv6 snooping policy** コマンドがイネーブルの場合、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変更されます。このモードでは、管理者が次の IPv6 ファーストホップセキュリティ コマンドを設定できます。

- **device-role** コマンドは、ポートに接続されているデバイスのロールを指定します。
- **limit address-count** *maximum* コマンドは、ポートで使用できる IPv6 アドレスの数を制限します。
- **protocol** コマンドは、アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定します。
- **security-level** コマンドは、適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーを上書きします。
- **trusted-port** コマンドは、ポートを信頼できるポートとして設定します。つまり、メッセージを受信したときに検証が限定的に実行されるか、まったく実行されません。

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# end
```

key chain macsec

事前共有キー（PSK）を取得するためにデバイスインターフェイスの MACsec キーチェーンの名前を設定するには、グローバル コンフィギュレーション モードで **key chain macsec** コマンドを使用します。CDP をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
key chain namemacsec
no key chain name [macsec ]
```

Syntax Description	<i>name</i> キーを取得するために使用するキーチェーンの名前。				
Command Default	key chain macsec は無効になっています。				
Command Modes	グローバル コンフィギュレーション (config)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

次に、128 ビットの事前共有キー（PSK）を取得するために MACsec キーチェーンを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 1000
Device(config-keychain-macsec)# cryptographic-algorithm aes-128-cmac
Device(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Device(config-keychain-macsec-key)# end
Device#
```

次に、256 ビットの事前共有キー（PSK）を取得するために MACsec キーチェーンを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 2000
Device(config-keychain-macsec)# cryptographic-algorithm aes-256-cmac
Device(config-keychain-macsec-key)# key-string c865632acb269022447c417504a1b
f5db1c296449b52627ba01f2ba2574c2878
Device(config-keychain-macsec-key)# end
Device#
```

key config-key password-encrypt

タイプ6の暗号キーをプライベートNVRAMに保存するには、グローバルコンフィギュレーションモードで **key config-key password-encrypt** コマンドを使用します。暗号化をディセーブルにするには、このコマンドの **no** 形式を使用します。

key config-key password-encrypt *text*
no key config-key password-encrypt *text*

Syntax Description

text (任意) Password または master キー。

Note 事前共有キーがどこにも出力されないようにするために、*text* 引数は使用せず、代わりにインタラクティブモードを使用 (**key config-key password-encrypt** コマンドを入力した後に **Enter** キーを使用) することを推奨します。

Command Default

タイプ6パスワード暗号キーはプライベートNVRAMに保存されません。

Command Modes

グローバルコンフィギュレーション (config)

Command History

リリース

Cisco IOS XE Fuji 16.9.2

変更

この
した。

Usage Guidelines

CLIを使用して、プレーンテキストのパスワードをタイプ6形式でNVRAMに安全に保存できます。タイプ6のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key password-encrypt** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます (キーの暗号化には対称キー暗号である高度暗号化規格 (AES) が使用されます)。**key config-key password-encrypt** コマンドを使用して設定されたパスワード (キー) は、デバイス内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key password-encrypt** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが設定されている起動時や不揮発性生成 (NVGEN) プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encrypt コマンドを使用してパスワード (マスターキー) が変更された場合、または再暗号化された場合には、リストレジストリから、タイプ6暗号が使用されているアプリケーションモジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

key config-key password-encrypt コマンドを使用して設定されたマスターキーがシステムから削除されると、タイプ 6 のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティ対策として、暗号化されたパスワードは、Cisco IOS ソフトウェアによって復号化されることはなくなります。ただし、すでに説明したように、パスワードを再暗号化することはできません。



Caution **key config-key password-encrypt** コマンドを使用して設定されたパスワードは、一度失われると回復できません。そのため、パスワードは安全な場所に保存しておくことを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encrypt** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号化できます。

パスワードの保存

（**key config-key password-encrypt** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、デバイスからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。その場合、パスワードは管理ステーション内部に安全に保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、デバイスにはロードできません。設定をデバイスにロードする前後には、（**key config-key password-encrypt** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できます。ただし、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカットアンドペーストした暗号文は、それがマスターキーに適合しない場合やマスターキーが存在しない場合でも、受理または保存されます。ただしこの場合にはアラートメッセージが表示されます。

```
"ciphertext>[for username bar] is incompatible with the configured master key."
```

マスターキーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ 6 のキーになります。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスターキーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encrypt** コマンドを使用してそのマスターキーを削除できます。マスターキーを削除しても、既存の暗号化パスワードは、暗号化された状態のままデバイス設定内に保持されます。これらのパスワードは復号化できません。

Examples

次に、タイプ 6 の暗号キーを NVRAM に保存する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# key config-key password-encrypt
```

Related Commands

コマンド	説明
password encryption aes	タイプ 6 の暗号化事前共有鍵を使用します。

key-server

MKA キーサーバオプションを設定するには、MKA ポリシー コンフィギュレーション モードで **key-server** コマンドを使用します。MKA キーサーバオプションを無効にするには、コマンドの **no** 形式を使用します。

key-server priority value
no key-server priority

Syntax Description	priority value	MKA キーサーバのプライオリティ値を指定します。
--------------------	----------------	---------------------------

Command Default MKA キーサーバは無効になっています。

Command Modes MKA ポリシー コンフィギュレーション (config-mka-policy)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、MKA キーサーバを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# key-server priority 33
```

Related Commands	Command	Description
	mka policy	MKA ポリシーを設定します。
	confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
	delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
	include-icv-indicator	MKPDU に ICV インジケータを含めます。
	macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
	sak-rekey	SAK キー再生成間隔を設定します。
	send-secure-announcements	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
	ssci-based-on-sci	SCI に基づいて SSCI を計算します。

Command	Description
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

limit address-count

ポートで使用できる IPv6 アドレスの数を制限するには、Neighbor Discovery Protocol (NDP) インスペクション ポリシー コンフィギュレーション モードまたは IPv6 スヌーピング コンフィギュレーション モードで **limit address-count** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

limit address-count *maximum*
no limit address-count

Syntax Description

maximum ポートで許可されているアドレスの数。範囲は 1 ~ 10000 です。

Command Default

デフォルト設定は無制限です。

Command Modes

IPv6 スヌーピング コンフィギュレーション (config-ipv6-snooping)
 ND インスペクション ポリシー コンフィギュレーション (config-nd-inspection)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

limit address-count コマンドは、ポリシーが適用されているポートで使用できる IPv6 アドレスの数を制限します。ポート上の IPv6 アドレスの数を制限すると、バインディング テーブル サイズの制限に役立ちます。範囲は 1 ~ 10000 です。

次に、NDP ポリシー名を `policy1` と定義し、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
Device(config-nd-inspection)# end
```

次に、IPv6 スヌーピングポリシー名を `policy1` と定義し、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
Device(config-ipv6-snooping)# end
```

local-domain (パラメータマップ)

Cisco Umbrella 統合機能のローカルドメインを設定するには、パラメータマップタイプ検査コンフィギュレーションモードで **local-domain** コマンドを使用します。ローカルドメインを削除するには、このコマンドの **no** 形式を使用します。

```
local-domain regex_param_map_name
no local-domain regex_param_map_name
```

Syntax Description	<i>regex_param_map_name</i>	正規表現パラメータマップの名前。
Command Default	パラメータマップのローカルドメインは作成されていません。	
Command Modes	パラメータマップタイプ検査コンフィギュレーション (config-profile)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。
Usage Guidelines	最大 64 のローカルドメインを設定できます。許可されるドメイン名の長さは 100 文字です。	
Examples	次に、ローカルドメインを設定する例を示します。	
	<pre>Device> enable Device# configure terminal Device(config)# parameter-map type umbrella global Device(config-profile)# local-domain dns_bypass</pre>	
Related Commands	コマンド	説明
	parameter-map type umbrella global	Umbrella モードでパラメータマップタイプを設定します。

mab logging verbose

MAC 認証バイパス (MAB) のシステムメッセージから詳細情報をフィルタリングするには、グローバル コンフィギュレーション モードで **mab logging verbose** コマンドを使用します。MAB システムメッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

mab logging verbose
no mab logging verbose

Syntax Description	このコマンドには引数またはキーワードはありません。	
Command Default	システムメッセージの詳細ログは有効になっていません。	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドにより、MAC 認証バイパス (MAB) システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
Device> enable
Device# configure terminal
Device(config)# mab logging verbose
Device(config)# exit
```

設定を確認するには、**show running-config** コマンドを入力します。

Related Commands	コマンド	説明
	authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングします。
	dot1x logging verbose	802.1X システムメッセージから詳細情報をフィルタリングしま
	mab logging verbose	MAC 認証バイパス (MAB) システムメッセージから詳細情報を タリングします。

mab request format attribute 32

デバイス上で VLAN ID ベースの MAC 認証をイネーブルにするには、グローバル コンフィギュレーションモードで **mab request format attribute 32 vlan access-vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan

Syntax Description

このコマンドには、引数またはキーワードはありません。

Command Default

VLAN-ID ベースの MAC 認証はディセーブルです。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。Microsoft IAS RADIUS サーバを使用したネットワークでこの機能を使用します。Cisco ACS はこのコマンドを無視します。

次に、デバイスで VLAN ID ベースの MAC 認証をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 32 vlan access-vlan
Device(config)# exit
```

Related Commands

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1X 認証をサポートしないクライアント用のフック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャモードを設定します。
authentication open	ポートでオープンアクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステータスの手動制御をイネーブルにします。

コマンド	説明
authentication priority	ポートプライオリティリストに認証方式を追加します。
authentication timer	802.1X 対応ポートのタイムアウトパラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでにデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC-based 認証をイネーブルにします。
mab eap	Extensible Authentication Protocol (EAP) を使用するようポートを設定します。
show authentication	デバイスの認証マネージャイベントに関する情報を表示します。

macsec-cipher-suite

Security Association Key (SAK) を取得するための暗号スイートを設定するには、MKA ポリシー コンフィギュレーションモードで **macsec-cipher-suite** コマンドを使用します。SAK の暗号スイートを無効にするには、このコマンドの **no** 形式を使用します。

macsec-cipher-suite gcm-aes-128
no macsec-cipher-suite gcm-aes-128

Syntax Description

gcm-aes-128 128 ビット暗号により SAK を取得するための暗号スイートを設定します。

Command Default

GCM-AES-128 暗号化は有効になっています。

Command Modes

MKA ポリシー コンフィギュレーション (config-mka-policy)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、128 ビット暗号化で SAK を取得するための MACsec 暗号スイートを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。

Command	Description
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

macsec network-link

アップリンク インターフェイスの MACsec Key Agreement (MKA) プロトコル設定を有効にするには、インターフェイス コンフィギュレーション モードで **macsec network-link** コマンドを使用します。CDP をディセーブルにするには、このコマンドの **no** 形式を使用します。

macsec network-link

no macsec network-link

Syntax Description	macsec network-link EAP-TLS 認証プロトコルを使用してデバイス インターフェイスの MKA MACsec 設定を有効にします。				
Command Default	macsec network-link は無効になっています。				
Command Modes	インターフェイス コンフィギュレーション (config-if)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

次に、EAP-TLS 認証プロトコルを使用して、インターフェイスに MACsec MKA を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/20
Device(config-if)# macsec network-link
Device(config-if)# end
Device#
```

match (アクセス マップ コンフィギュレーション)

VLAN マップを1つまたは複数のアクセス リストとパケットを照合するように設定するには、アクセスマップコンフィギュレーションモードで**match**コマンドを使用します。一致パラメータを削除するには、このコマンドの**no**形式を使用します。

```
match {ip address {namenumber} [namenumber] [namenumber]... | ipv6 address {namenumber}
[namenumber] [namenumber]... | mac address {name} [name] [name]...}
no match {ip address {namenumber} [namenumber] [namenumber]... | ipv6 address
{namenumber} [namenumber] [namenumber]... | mac address {name} [name] [name]...}
```

Syntax Description	
ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
ipv6 address	パケットを IPv6 アドレス アクセス リストと照合するようにアクセス マップを設定します。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
<i>name</i>	パケットを照合するアクセス リストの名前です。
<i>number</i>	パケットを照合するアクセス リストの番号です。このオプションは、MAC アクセス リストに対しては無効です。

Command Default デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

Command Modes アクセスマップ コンフィギュレーション (config-access-map)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **vlan access-map** グローバル コンフィギュレーション コマンドを使用して、アクセスマップ コンフィギュレーション モードを開始します。

1つのアクセス リストの名前または番号を入力する必要があります。その他は任意です。パケットは、1つまたは複数のアクセス リストに対して照合できます。いずれかのリストに一致すると、エントリの一致としてカウントされます。

アクセスマップコンフィギュレーションモードでは、**match**コマンドを使用して、VLANに適用される VLAN マップの一致条件を定義できます。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

パケットは、同じプロトコル タイプのアクセス リストに対してだけ照合されます。IP パケットは、IP アクセス リストに対して照合され、IPv6 パケットは IPv6 アクセス リストに対して照合され、その他のパケットはすべて MAC アクセス リストに対して照合されます。

同じマップ エントリに、IP アドレス、IPv6 アドレスおよび MAC アドレスを指定できます。

Examples

次の例では、VLAN アクセス マップ `vmap4` を定義して VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト `al2` に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
Device> enable
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
Device(config)# exit
```

設定を確認するには、`show vlan access-map` コマンドを入力します。

mka pre-shared-key

事前共有キー（PSK）を使用してデバイスインターフェイスの MACsec Key Agreement（MKA）MACsec を設定するには、グローバル コンフィギュレーション モードで **mka pre-shared-key key-chain *key-chain name*** コマンドを使用します。CDP をディセーブルにするには、このコマンドの **no** 形式を使用します。

mka pre-shared-key key-chain *key-chain-name*
no mka pre-shared-key key-chain *key-chain-name*

Syntax Description	mka pre-shared-key key-chain PSK を使用してデバイス インターフェイスの MACsec MKA 設定を有効にします。				
Command Default	mka pre-shared-key はディセーブルです。				
Command Modes	インターフェイス コンフィギュレーション (config-if)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

次に、PSK を使用して、インターフェイスの MKA MACsec を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/20
Device(config-if)# mka pre-shared-key key-chain kcl
Device(config-if)# end
Device#
```

mka suppress syslogs sak-rekey

ロギングにおいて MACsec Key Agreement (MKA) セキュア アソシエーション キー (SAK) のキー再生成メッセージを抑制するには、グローバルコンフィギュレーションモードで **mka suppress syslogs sak-rekey** コマンドを使用します。MKA SAK キー再生成メッセージのロギングを無効にするには、このコマンドの **no** 形式を使用します。

mka suppress syslogs sak-rekey
no mka suppress syslogs sak-rekey

このコマンドには引数またはキーワードはありません。

Command Default

すべての MKA SAK syslog メッセージがコンソールに表示されます。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.9.1	このコマンドが導入されました。

Usage Guidelines

MKA SAK syslog はすべてのキー再生成間隔で継続的に生成されるため、複数のインターフェイスで MKA が設定されている場合は生成される syslog の量が非常に多くなります。MKA SAK syslog を抑制するには、このコマンドを使用します。

例

次に、MKA SAK syslog ロギングを抑制する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka suppress syslogs sak-rekey
```

parameter-map type regex

正規表現を使用して特定のトラフィックパターンを照合するパラメータマップタイプを設定するには、グローバル コンフィギュレーション モードで **parameter-map type regex** コマンドを使用します。正規表現を使用したパラメータマップタイプを削除するには、このコマンドの **no** 形式を使用します。

parameter-map type regex *parameter-map-name*
no parameter-map type regex

Syntax Description

parameter-map-name パラメータ マップの名前。この名前には最大 228 文字までの英数字を指定できます。

Note 空白を使用することは推奨されません。文字列が引用符で区切られていない限り、システムは最初の空白をパラメータマップ名の末尾と解釈します。

Command Default

正規表現パラメータマップは設定されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines

正規表現では、テキスト文字列を文字列そのものとして照合することも、メタ文字を使用してテキスト文字列の複数のバリエーションと照合することもできます。正規表現を使用して、特定のアプリケーショントラフィックの内容を照合できます。たとえば、HTTP インспекション クラス マップの **match request regex** コマンドを使用すると、HTTP パケット内の Uniform Resource Identifier (URI) 文字列を照合できます。

Ctrl+V を押すと、CLI において、疑問符 (?) やタブなどの特殊文字がすべて無視されます。たとえば、設定で **d?g** と入力するには、**d[Ctrl-V]g** とキー入力します。

次の表に、特別な意味を持つメタ文字を示します。

Table 145: regex メタ文字

文字	説明	注意
.	ドット	任意の単一文字と一致します。たとえば、 d.g は、dog、dag、dtg、およびこれらの文字を含む任意の単語に一致します。

文字	説明	注意
(xxx)	サブ表現	文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、 d(o a)g は dog および dag に一致しますが、 do ag は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、 ab(xy){3}z は、 abxyxyxyz に一致します。
	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、 dog cat は、 dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示します。たとえば、 lo?se は、 lse または lose に一致します。 Note 疑問符の前に Ctrl+V を入力する必要があります。そうしないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示します。たとえば、 lo*se は、 lse 、 lose 、 loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示します。たとえば、 lo+se は、 lose および loose に一致しますが、 lse には一致しません。
{ 〇 }	繰り返し限定作用素	厳密に x 回繰り返します。たとえば、 ab(xy){3}z は、 abxyxyxyz に一致します。
{ 〇 , }	最小繰り返し限定作用素	少なくとも x 回繰り返します。たとえば、 ab(xy){2,}z は、 abxyxyz や abxyxyxyz などに一致します。
[abc]	文字クラス	角カッコ内の任意の文字と一致します。たとえば、 [abc] は、 a 、 b 、または c に一致します。
[^ abc]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、 [^abc] は a 、 b 、 c 以外の任意の文字に一致し、 [^A-Z] は大文字以外の任意の 1 文字に一致します。
[a - c]	文字範囲クラス	指定した範囲内の任意の文字と一致します。 [a-z] は、任意の小文字と一致します。文字と範囲を組み合わせることもできます。たとえば、 [abcq-z] および [a-cq-z] は、 a 、 b 、 c 、 q 、 r 、 s 、 t 、 u 、 v 、 w 、 x 、 y 、 z に一致します。 Note ダッシュ (-) 文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります ([abc-] や [-abc])。

文字	説明	注意
“”	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、"test" は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	リテラル文字の前にある場合、リテラル文字と一致します。たとえば、\[は左角カッコに一致します。
<i>char</i>	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォームフィード 0x0c と一致します。
\x <i>nn</i>	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
\ <i>nnn</i>	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

Examples

次に、URI が次の正規表現のいずれかと一致する正規表現パラメータマップを設定して HTTP アプリケーション ファイアウォールパラメータマップタイプに適用する例を示します。

- ".*cmd.exe"
- ".*money"
- ".*shopping"

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex uri-regex-cm
Device(config-profile)# pattern ".*cmd.exe"
Device(config-profile)# pattern ".*money"
Device(config-profile)# pattern ".*shopping"
Device(config-profile)# exit
Device(config)# class-map type inspect http uri-check-cm
Device(config-cmap)# match request uri regex uri-regex-cm
Device(config-cmap)# exit
Device(config)# policy-map type inspect http uri-check-pm
Device(config-pmap)# class type inspect http uri-check-cm
Device(config-pmap-c)# reset
```

次に、文字列 hello の複数のバリエーションと一致する大文字と小文字を区別しないパターンの正規表現パラメータマップを設定する例を示します。

```

Device# configure terminal
Device(config)# parameter-map type regex body_regex
Device(config-profile)# pattern ".*[Hh][Ee][Ll][Ll][Oo]"
Device(config-profile)# end

```

Related Commands

コマンド	説明
class-map type inspect	レイヤ3とレイヤ4またはレイヤ7（アプリケーション固有）の検査タイプクラスマップを作成します。
class type inspect	アクションが実行されるトラフィック（クラス）を指定します。
match request regex	要求メッセージのURIまたは引数（パラメータ）が定義された正規表現と一致しているかどうかに基づいてHTTPトラフィックを許可または拒否するHTTPファイアウォールポリシーを設定します。
parameter-map type	パラメータマップを作成または変更します。
policy-map type inspect	レイヤ3とレイヤ4またはレイヤ7（アプリケーション固有）の検査タイプポリシーマップを作成します。

parameter-map type umbrella global

Umbrella モードのパラメータマップタイプを設定するには、グローバル コンフィギュレーション モードで **parameter-map type umbrella global** コマンドを使用します。Umbrella モードのパラメータマップタイプを削除するには、このコマンドの **no** 形式を使用します。

parameter-map type umbrella global
no parameter-map type umbrella

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default Umbrella モードのパラメータマップは設定されていません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、パラメータマップタイプを Umbrella モードに設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)#
```

Related Commands

コマンド	説明
parameter-map type	パラメータマップを作成または変更します。

password encryption aes

タイプ 6 の暗号化事前共有キーをイネーブルにするには、グローバル コンフィギュレーション モードで **password encryption aes** コマンドを使用します。パスワードの暗号化をディセーブルにするには、このコマンドの **no** 形式を使用します。

password encryption aes
no password encryption aes

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

事前共有キーは暗号化されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース

Cisco IOS XE Fuji 16.9.2

変更

この
した。

Usage Guidelines

CLI を使用して、プレーンテキストのパスワードをタイプ 6 形式で NVRAM に安全に保存できます。タイプ 6 のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key password-encrypt** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます（キーの暗号化には対称キー暗号である高度暗号化規格（AES）が使用されます）。**key config-key password-encrypt** コマンドを使用して設定されたパスワード（キー）は、ルータ内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key password-encrypt** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが実行される起動時や不揮発性生成（NVGEN）プロセス中に次のようなメッセージが出力されません。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encrypt コマンドを使用してパスワード（マスターキー）が変更された場合、または再暗号化された場合には、リストレジストリから、タイプ 6 暗号が使用されているアプリケーションモジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

key config-key password-encrypt コマンドを使用して設定されたマスターキーがシステムから削除されると、タイプ 6 のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティ対策として、暗号化されたパスワード

ドは、Cisco IOS ソフトウェアによって復号化されることはなくなります。ただし、すでに説明したように、パスワードを再暗号化することはできません。



Caution **key config-key password-encrypt** コマンドを使用して設定されたパスワードは、一度失われると回復できません。そのため、パスワードは安全な場所に保存しておくことを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encrypt** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号化できます。

パスワードの保存

（**key config-key password-encrypt** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、ルータからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。そのため、パスワードは管理システム内部に安全に保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、ルータにはロードできません。設定をルータにロードする前後には、（**key config-key password-encrypt** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できますが、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカットアンドペーストした暗号文は、それがマスターキーに適合しない場合やマスターキーが存在しない場合でも、受理または保存されます。ただしこの場合には次のアラートメッセージが表示されます。

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

マスターキーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ 6 のキーに変換されます。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスターキーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encrypt** コマンドを使用してそのマスターキーを削除できます。既存の暗号化パスワードは、暗号化された状態のままルータ設定内に保持されます。これらのパスワードは復号化されません。

Examples

次に、タイプ 6 の暗号化事前共有キーをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device (config)# password encryption aes
```

Related Commands

コマンド	説明
key config-key password-encrypt	タイプ6の暗号キーをプラットフォームに保存します。

pattern (パラメータマップ)

ローカルURLフィルタリングで許可またはブロックする必要があるドメイン、URL キーワード、または URL メタ文字のリストを指定する照合パターンを設定するには、パラメータマップタイプ検査コンフィギュレーションモードで **pattern** コマンドを使用します。照合パターンを削除するには、このコマンドの **no** 形式を使用します。

pattern *expression*
no pattern *expression*

Syntax Description	<i>expression</i>	ドメイン名、URL キーワード、URL メタ文字のエントリ、または URL キーワードとメタ文字の組み合わせを参照する照合パターン引数。
Command Default	パラメータマップのパターンは作成されていません。	
Command Modes	パラメータマップタイプ検査コンフィギュレーション (config-profile)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines 照合パターン表現は、**parameter-map type regex** コマンドで作成されたパラメータマップに対して設定されます。

パターン表現では、文字 /、{、} は使用できません。疑問符 (?) 文字は、CLI ヘルプ機能用に予約されているため使用できません。アスタリスク (*) 文字は、パターンの先頭には使用できません。

URL パターンマッチングでは、ピリオド (.) 文字はドットとして解釈され、単一の文字を表すワイルドカードエントリとしては解釈されません。これは、正規表現パターンマッチングの場合と同じです。URL フィルタリングでは、ホスト名またはドメイン名に任意の文字が含まれる場合にそれらを許可またはブロックできます。

URL キーワードは、ドメイン名の後のパスに含まれるスラッシュ (/) で区切られたひとかたまりの語句です。たとえば、URL `http://www.example.com/hack/123.html` では、**hack** のみがキーワードとして扱われます。URL 内のキーワード全体がパターンと一致している必要があります。たとえば、**hack** というパターンを設定した場合、URL `www.example.com/hacksite/123.html` はパターンと一致しません。この URL を一致させるには、パターンに **hacksite** を含める必要があります。

URL メタ文字を使用すると、UNIX の glob 表現のように、パターンマッチングで URL の単一の文字または文字の範囲を照合できます。URL メタ文字を次の表に示します。

Table 146: URL パターンマッチングの URL メタ文字

文字	説明
*	アスタリスク: 0 文字以上の任意のシーケンスと一致します。
[abc]	文字クラス: 各カッコ内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。たとえば、[abc] は、a、b、または c に一致します。
[a-c]	文字範囲クラス: 指定した範囲内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。たとえば、[a-z] は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。たとえば、[abcq-z] および [a-cq-z] は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 Note ダッシュ (-) 文字は、角カッコ内の最初の文字または最後の文字である場合にのみ照合されます ([abc-] や [-abc])。
[0-9]	数字範囲クラス: 各カッコ内の任意の数字と一致します。たとえば、[0-9] は、0、1、2、3、4、5、6、7、8、9 に一致します。

URL メタ文字をドメイン名や URL キーワードと組み合わせてパターンマッチングに使用できます。たとえば、www.example[0-9][0-9].com というパターンを使用すると、www.example01.com、www.example33.com、www.example99.comなどをブロックできます。キーワードとメタ文字を組み合わせて、URL をブロックする照合パターンを作成できます。たとえば、hack* というパターンを使用すると、www.example.com/hacksite/123.html をブロックできます。

parameter-map type regex コマンドを設定してから **pattern** コマンドを設定すると、**pattern** コマンドで指定したパターンが General Packet Radio Service (GPRS) トンネリングプロトコル (GTP) クラスのフィルタとして使用されます。

Examples

次に、指定した URL を照合するパターンを設定する例を示します。

```
Device(config)# parameter-map type regex dns_bypass
Device(config-profile)# pattern www.example.com
```

次に、文字列 hello の複数のバリエーションと一致する大文字と小文字を区別しないパターンを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex body-regex
Device(config-profile)# pattern ".*[Hh][Ee][Ll][Ll][Oo]"
```

次の例は、パターンの先頭にアスタリスク (*) 文字が指定されている場合にコンソールに表示されるエラーメッセージを示しています。

pattern (パラメータマップ)

```
Device(config)# parameter-map type regex gtp-map
Device(config-profile)# pattern *.gprs.com
%Invalid first char + or * in regex pattern
```

Related Commands

コマンド	説明
parameter-map type regex	特定の正規表現パターンを照合する正規表現パラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーションモードを開始します。

permit (MAC アクセス リスト コンフィギュレーション)

条件が一致した場合に非 IP トラフィックの転送を許可するには、MAC アクセスリスト コンフィギュレーションモードで **permit** コマンドを使用します。拡張 MAC アクセスリストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

```
{permit {any | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | ladv-sca | lsap|sap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
nopermit {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | ladv-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]}
```

Syntax Description

any	すべての送信元または宛先 MAC アドレスを拒否
host <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>	ホスト MAC アドレスと任意のサブネットマスクが定義されたアドレスに一致する場合、そのアドレスを許可します。
host <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>	宛先 MAC アドレスと任意のサブネットマスクを定義されたアドレスに一致する場合、そのアドレスを許可します。
<i>type mask</i>	(任意) パケットの EtherType 番号と、Ethernet パケットのプロトコルを識別します。 <ul style="list-style-type: none"> • <i>type</i> には、0 ~ 65535 の 16 進数を指定できます。 • <i>mask</i> は、一致をテストする前に EtherType に一致する必要があります。
aarp	(任意) データリンクアドレスをネットワークアドレス Resolution Protocol を指定します。
amber	(任意) EtherType DEC-Amber を指定します。
appletalk	(任意) EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	(任意) EtherType Digital Equipment Corporation を指定します。
decnet-iv	(任意) EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	(任意) EtherType DEC-Diagnostic を指定します。
dsm	(任意) EtherType DEC-DSM を指定します。
etype-6000	(任意) EtherType 0x6000 を指定します。
etype-8042	(任意) EtherType 0x8042 を指定します。

lat	(任意) EtherType DEC-LAT を指定します。
lavc-sca	(任意) EtherType DEC-LAVC-SCA を指定します。
lsap <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と 802.1Q プロトコルを指定します。 <i>mask</i> は、一致をテストする前に LSAP 番号に適用されます。
mop-console	(任意) EtherType DEC-MOP Remote Console を指定します。
mop-dump	(任意) EtherType DEC-MOP Dump を指定します。
msdos	(任意) EtherType DEC-MSDOS を指定します。
mumps	(任意) EtherType DEC-MUMPS を指定します。
netbios	(任意) EtherType DEC-Network Basic Input/Output System を指定します。
vines-echo	(任意) Banyan Systems による EtherType Virtual Interface Protocol を指定します。
vines-ip	(任意) EtherType VINES IP を指定します。
xns-idp	(任意) EtherType Xerox Network Systems (XNS) Protocol を指定します。
cos <i>cos</i>	(任意) プライオリティを設定するため、0 ~ 7 を指定します。CoSに基づくフィルタリングは、ハードウェアが設定されているかどうかを確認する警告メッセージを生成します。

Command Default このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

Command Modes MAC アクセス リスト コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **appletalk** は、コマンドラインのヘルプストリングには表示されますが、一致条件としてはサポートされていません。

mac access-list extended グローバル コンフィギュレーション コマンドを使用して、MAC アクセス リスト コンフィギュレーション モードを開始します。

host キーワードを使用した場合、アドレスマスクは入力できません。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセスコントロールエントリ (ACE) がアクセスコントロールリストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap lsap mask** キーワードを使用します。Novell 用語と Cisco IOS XE 用語での IPX カプセル化タイプに対応するフィルタ条件を、次の表に一覧表示します。

Table 147: IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novell 名	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa への NetBIOS トラフィックを許可する名前付き MAC 拡張アクセスリストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
Device(config-ext-macl)# end
```

次の例では、名前付き MAC 拡張アクセスリストから許可条件を削除する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
Device(config-ext-macl)# end
```

次の例では、EtherType 0x4321 のすべてのパケットを許可します。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any any 0x4321 0
Device(config-ext-macl)# end
```

設定を確認するには、**show access-lists** コマンドを入力します。

Related Commands

コマンド	説明
deny	MAC アクセスリストを拒否します。条件が満たされるとパケットが転送されるのを拒否します。
mac access-list extended	非 IP トラフィック用の MAC アクセスリストを作成します。
show access-lists	デバイスに設定されたアクセスリストを表示します。

protocol (IPv6 スヌーピング)

s

アドレスを Dynamic Host Configuration Protocol (DHCP) または Neighbor Discovery Protocol (NDP) で収集する必要があることを指定するか、プロトコルを IPv6 プレフィックスリストに対応させるには、IPv6 スヌーピング コンフィギュレーションモードで **protocol** コマンドを使用します。DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
protocol {dhcp | ndp}
no protocol {dhcp | ndp}
```

Syntax Description

dhcp アドレスをダイナミック ホスト コンフィギュレーションプロトコル (DHCP) パケットで収集する必要があることを指定します。

ndp アドレスをネイバー探索プロトコル (NDP) パケットで収集する必要があることを指定します。

Command Default

スヌーピングとリカバリは DHCP および NDP の両方を使用して試行します。

Command Modes

IPv6 スヌーピング コンフィギュレーションモード (config-ipv6-snooping)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

アドレスが DHCP または NDP に関連付けられたプレフィックスリストと一致しない場合は、制御パケットがドロップされ、バインディングテーブルエントリのリカバリはそのプロトコルに対しては試行されません。

- **no protocol {dhcp | ndp}** コマンドを使用すると、プロトコルはスヌーピングまたはグリーンングに使用されません。
- **no protocol dhcp** コマンドを使用すると、DHCP は依然としてバインディングテーブルのリカバリに使用できます。
- データ収集は DHCP および NDP でリカバリできますが、宛先ガードは DHCP によるのみリカバリできます。

次に、IPv6 スヌーピングポリシー名を `policy1` と定義し、アドレスの収集に DHCP を使用するようにポートを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
```

```
Device (config-ipv6-snooping) # protocol dhcp
Device (config-ipv6-snooping) # end
```

radius server

RADIUS アカウンティングと RADIUS 認証を含む RADIUS サーバのパラメータを設定するには、グローバルコンフィギュレーションモードで **radius server** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
radius server name
address {ipv4 | ipv6} ip{address / hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

Syntax Description

address {ipv4 ipv6} <i>ip{address / hostname}</i>	RADIUS サーバの IP アドレスを指定します。
auth-port <i>udp-port</i>	(任意) RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
acct-port <i>udp-port</i>	(任意) RADIUS アカウンティングサーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
key <i>string</i>	(任意) デバイスと RADIUS デーモン間のすべての RADIUS 通信の認証キーおよび暗号キーを指定します。 Note キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。必ずこのコマンドの最終項目として key を設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。key にスペースが含まれる場合は、引用符が key の一部でない限り、 key を引用符で囲まないでください。
automate tester <i>name</i>	(任意) RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定します。
retransmit <i>value</i>	(任意) サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ～ 100 です。この設定は、 radius-server retransmit グローバルコンフィギュレーションコマンドによる設定を上書きします。
timeout <i>seconds</i>	(任意) device が要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ～ 1000 です。この設定は radius-server timeout コマンドを上書きします。

Command Default

- RADIUS アカウンティングサーバの UDP ポートは 1646 です。
- RADIUS 認証サーバの UDP ポートは 1645 です。
- 自動サーバテストはディセーブルです。

- タイムアウトは 60 分（1 時間）です。
- 自動テストがイネーブルの場合、UDP ポートのアカウントिंगおよび認証時にテストが実行されます。
- 認証キーおよび暗号キー（string）は設定されていません。

Command Modes グローバル コンフィギュレーション（config）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

- Usage Guidelines**
- RADIUS アカウントिंग サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。
 - RADIUS サーバ コンフィギュレーション モードで **key string** コマンドを使用すると、認証および暗号キーを設定できます。必ずこのコマンドの最終項目として **key** を設定してください。
 - RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定するには、**automate-tester name** キーワードを使用します。

次の例では、認証サーバの UDP ポートを 1645、アカウントングサーバの UDP ポートを 1646 に設定し、文字列を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
Device(config-radius-server)# end
```

radius-server dead-criteria

RADIUS サーバを **dead** としてマークするために使用する基準のいずれかまたは両方を示されている定数に強制的に設定するには、**radius-server dead-criteria** コマンドをグローバル コンフィギュレーション モードで使用します。設定されていた基準を無効にするには、このコマンドの **no** 形式を使用します。

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]
no radius-server dead-criteria [**time** *seconds* | **tries** *number-of-tries*]

Syntax Description

time <i>seconds</i>	<p>(任意) デバイスが RADIUS サーバから有効なパケットを最後に受信してから、サーバが dead としてマークされるまでに経過する必要がある最小時間 (秒単位)。デバイスの起動後にパケットを受信せずにタイムアウトになった場合は、この時間の条件は満たされたものとして処理されます。この時間は 1 ~ 120 秒に設定できます。</p> <ul style="list-style-type: none"> • <i>seconds</i> 引数を設定しない場合、この秒数はサーバのトランザクションレートに応じて 10 ~ 60 秒になります。 <p>Note 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。</p>
tries <i>number-of-tries</i>	<p>(任意) RADIUS サーバが dead としてマークされるまでにデバイスで発生する必要がある連続タイムアウト回数。サーバが認証とアカウントの両方を実行する場合、両方の種類のパケットがこの回数に含まれます。正しく作成されていないパケットは、タイムアウトになっているものとしてカウントされます。最初の送信と再送信を含むすべての送信がカウントされます。タイムアウト回数は 1 ~ 100 に設定できます。</p> <ul style="list-style-type: none"> • <i>number-of-tries</i> 引数を設定しない場合、連続タイムアウト回数はサーバのトランザクションレートと設定されている再送信回数に基づいて 10 ~ 100 となります。 <p>Note 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。</p>

Command Default

RADIUS サーバがデッド状態としてマークされるまでに発生する連続タイムアウトの回数と秒数は、サーバのトランザクション レートと設定されている再送信回数に応じて異なります。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines



Note 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

このコマンドの **no** 形式では、次のようになります。

- *number-of-tries* 引数も *seconds* 引数も **no radius-server dead-criteria** コマンドに指定されていない場合は、時間と試行回数の両方がそれらのデフォルトにリセットされます。
- 最初に設定されていた値を使用して *seconds* 引数が指定された場合、時間はデフォルトの値範囲（10 ～ 60）にリセットされます。
- 最初に設定されていた値を使用して *number-of-tries* 引数が指定された場合、時間はデフォルトの値範囲（10 ～ 100）にリセットされます。

Examples

次に、5 秒が経過して 4 回の試行後にデバイスが **dead** と見なされるようにデバイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 5 tries 4
```

次に、**radius-server dead-criteria** コマンドに設定されていた時間と試行回数の基準を無効にする例を示します。

```
Device(config)# no radius-server dead-criteria
```

次に、**radius-server dead-criteria** コマンドに設定されていた時間の基準を無効にする例を示します。

```
Device(config)# no radius-server dead-criteria time 5
```

次に、**radius-server dead-criteria** コマンドに設定されていた試行回数の基準を無効にする例を示します。

```
Device(config)# no radius-server dead-criteria tries 4
```

Related Commands

Command	Description
debug aaa dead-criteria transactions	デッド条件の AAA トランザクションの値を表示します。
show aaa dead-criteria	AAA サーバのデッド条件に関する情報を表示します。
show aaa server-private	すべてのプライベート RADIUS サーバのステータスを表示します。
show aaa servers	AAA サーバとの間で送受信されたパケットの数に関する情報を表示します。

radius-server deadline

一部のサーバが使用不能な場合の RADIUS 応答時間を改善し、使用不能なサーバを即時にスキップするには、**radius-server deadline** コマンドをグローバルコンフィギュレーションモードで使用します。deadline を 0 に設定するには、このコマンドの **no** 形式を使用します。

radius-server deadline minutes
no radius-server deadline

Syntax Description	<i>minutes</i>	トランザクション要求が RADIUS サーバをスキップする期間（分単位、最大 1440 分（24 時間））。
---------------------------	----------------	--

Command Default デッドタイムは 0 に設定されます。

Command Modes グローバル コンフィギュレーション（config）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、Cisco IOS ソフトウェアが認証要求に応答しない RADIUS サーバを *dead* としてマークできるようにします。これにより、設定されている次のサーバを試行する前に要求の待機がタイムアウトになることが防止されます。*dead* としてマークされた RADIUS サーバは、指定された期間（分単位）、その他の要求でスキップされます。ただし、*dead* としてマークされていないサーバが他にない場合を除きます。



Note *dead* としてマークされた RADIUS サーバが誘導要求を受信する場合、その誘導要求は RADIUS サーバで除外されません。ダイレクト要求は RADIUS サーバに直接送信されるため、RADIUS サーバはダイレクト要求の処理を続行します。

次の両方の条件を満たした場合に RADIUS サーバが *dead* としてマークされます。

1. サーバへ再送信するかどうかを決定するために使用される最小限のタイムアウト期間内に、未処理のトランザクションに対する有効な応答を RADIUS サーバから受信しなかった。
2. 最小限必要な再送信回数に 1（初回送信分）を加算した回数だけ、パケットがすべてのトランザクションで連続して RADIUS サーバに送信されたが、必要なタイムアウト期間内にサーバから有効な応答を受信しなかった。

Examples

次に、認証要求への応答に失敗した RADIUS サーバのデッドタイムを 5 分に指定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius-server deadtime 5

```

Related Commands

Command	Description
deadtime (server-group configuration)	RADIUS サーバグループのコンテキスト内でデッドタイムを設定します。
radius-server host	RADIUS サーバホストを指定します。
radius-server retransmit	Cisco IOS ソフトウェアが RADIUS サーバホストのリストを検索する回数の最大値を指定します。
radius-server timeout	サーバホストが応答するまでデバイスが待機する間隔を設定します。

radius-server directed-request

ユーザがシスコのネットワークアクセスサーバ（NAS）にログインして認証用の RADIUS サーバを選択できるようにするには、**radius-server directed-request** コマンドをグローバルコンフィギュレーションモードで使用します。誘導要求機能を無効にするには、このコマンドの **no** を使用します。

```
radius-server directed-request [restricted]
no radius-server directed-request [restricted]
```

Syntax Description

restricted	（任意）指定したサーバが使用できない場合、ユーザがセカンダリサーバに送信されないようにします。
-------------------	---

Command Default

ユーザはシスコの NAS にログインできないため、認証用の RADIUS サーバを選択します。

Command Modes

グローバル コンフィギュレーション（config）

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

radius-server directed-request コマンドは、「@」記号より前のユーザ名の部分のみを「@」記号の後に指定したホストに送信します。つまり、このコマンドを有効にすると、設定済みのサーバのいずれにも要求を送信でき、ユーザ名のみが指定したサーバに送信されます。



Note **server-private**（RADIUS）コマンドを設定してプライベート RADIUS サーバをグループサーバとして使用した場合は、**radius-server directed-request** コマンドを設定することはできません。

次に、RADIUS サーバにメッセージを送信する一連のイベントを示します。

- **radius-server directed-request** コマンドを設定した場合は、次のようになります。
 - 要求が誘導先のサーバに送信されます。同じ IP アドレスを持つサーバが複数ある場合、要求は同じ IP アドレスを持つ最初のサーバにのみ送信されます。
 - 応答を受信しない場合、要求は最初の方式リストに示されているすべてのサーバに送信されます。
 - 最初の方式で応答を受信しなかった場合、要求は方式リストの最後に到達するまで、2 番目の方式リストに示されているすべてのサーバに送信されます。



Note 誘導先のサーバを選択するには、指定された要求に指定された IP アドレスを持つサーバの方式リスト内の最初のサーバグループを検索します。使用できない場合、グローバルプールの同じ IP アドレスを持つ最初のサーバグループが考慮されます。

- **radius-server directed-request restricted** コマンドを方式リスト内のすべてのサーバグループに対して設定した場合、誘導先のサーバから応答を受信するまで、または方式リストの最後に到達するまで、次のアクションが実行されます。
 - 誘導先のサーバの IP アドレスを持つ最初のサーバを使用して要求が送信されます。
 - 同じ IP アドレスを持つサーバがサーバグループ内に見つからない場合は、誘導先のサーバの IP アドレスを持つグローバルプール内の最初のサーバが使用されます。

radius-server directed-request コマンドを **no radius-server directed-request** コマンドを使用して無効にした場合、文字列全体（「@」記号の前と後ろの両方）がデフォルトの RADIUS サーバに送信されます。ルータは、リスト内の最初のサーバから順にサーバのリストを照会します。文字列全体を送信し、サーバからの最初の応答を受け入れます。

ユーザをユーザ名の一部として識別された RADIUS サーバに制限するには、**radius-server directed-request restricted** コマンドを使用します。

ユーザ要求にサーバ IP アドレスがある場合、誘導先のサーバはその要求をグループに転送する前に特定のサーバに転送します。たとえば、`user@10.0.0.1` などのユーザ要求が誘導先のサーバに送信され、このユーザ要求に指定されている IP アドレスがサーバの IP アドレスの場合、誘導先のサーバはユーザ要求を特定のサーバに転送します。

誘導先のサーバがサーバグループとホストサーバの両方に設定されている場合に設定したサーバ名を持つユーザ要求が誘導先のサーバに送信されると、誘導先のサーバはユーザ要求をサーバグループに転送する前にホストサーバに転送します。たとえば、`user@10.0.0.1` というユーザ要求が誘導先のサーバに送信され、`10.0.0.1` がホストサーバのアドレスである場合、誘導先のサーバはユーザ要求をサーバグループに転送する前に、ホストサーバに転送します。



Note **no radius-server directed-request restricted** コマンドを入力すると、`restricted` フラグのみが削除され、`directed-request` フラグは保持されます。誘導要求機能を無効にするには、**no radius-server directed-request** コマンドも入力する必要があります。

Examples

次に、誘導要求機能を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# radius server rad-1
Device(config-radius-server)# address ipv4 10.1.1.2
Device(config-radius-server)# key dummy123
Device(config-radius-server)# exit
Device(config)# radius-server directed-request
```

Related Commands

Command	Description
aaa group server	各種のサーバホストを別個のリストと別個の方式にグループ化します。
aaa new-model	AAA アクセスコントロールモデルをイネーブルにします。
server-private (RADIUS)	グループサーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

radius-server domain-stripping

ユーザ名をリモート RADIUS サーバに転送する前にユーザ名からサフィックスをストリッピングするか、またはサフィックスとプレフィックスの両方をストリッピングするようにネットワークアクセスサーバ (NAS) を設定するには、**radius-server domain-stripping** コマンドをグローバルコンフィギュレーションモードで使用します。ストリッピング設定を無効にするには、このコマンドの **no** 形式を使用します。



Note デフォルトの vrf 名が設定されるまでにデフォルトの VRF 名が確実に NULL 値になるように、**ip vrf default** コマンドをグローバルコンフィギュレーションモードで設定してから **radius-server domain-stripping** コマンドを設定する必要があります。

```
radius-server domain-stripping [ [right-to-left] [prefix-delimiter character [character2 . . . character7]] [delimiter character [character2 . . . character7]] |strip-suffix suffix ] [vrf vrf-name ]
no radius-server domain-stripping [ [right-to-left] [prefix-delimiter character [character2 . . . character7]] [delimiter character [character2 . . . character7]] |strip-suffix suffix ] [vrf vrf-name ]
```

Syntax Description

right-to-left	(任意) 完全なユーザ名を右から左に解析するときに検出された最初のデリミタで NAS がストリッピング設定を適用するように指定します。デフォルトでは、NAS は、完全なユーザ名を左から右に解析するときに検出された最初のデリミタでストリッピング設定を適用します。
prefix-delimiter <i>character</i> [<i>character2...character7</i>]	(任意) プレフィックスのストリッピングを有効にし、プレフィックスデリミタとして認識される 1 つまたは複数の文字を指定します。 <i>character</i> 引数の有効な値は @、/、\$、%、\、# と - です。スペースを挟むことなく複数の文字を入力できます。プレフィックスデリミタとして 7 文字までを定義できます。これが有効な文字の最大数です。 <i>character</i> 引数の最後の文字または唯一の文字として \ を入力する場合は、\\ と入力する必要があります。デフォルトでは、プレフィックスデリミタは定義されていません。
delimiter <i>character</i> [<i>character2...character7</i>]	(任意) サフィックスデリミタとして認識される 1 つまたは複数の文字を指定します。 <i>character</i> 引数の有効な値は @、/、\$、%、\、# と - です。スペースを挟むことなく複数の文字を入力できます。サフィックスデリミタとして最大 7 文字を定義できます。これが有効な文字の最大数です。 <i>character</i> 引数の最後の文字または唯一の文字として \ を入力する場合は、\\ と入力する必要があります。デフォルトのサフィックスデリミタは @ 文字です。
strip-suffix <i>suffix</i>	(任意) ユーザ名から削除するサフィックスを指定します。

vrf <i>vrf-name</i>	(任意) ドメインストリッピング設定をバーチャルプライベートネットワーク (VPN) ルーティングおよび転送 (VRF) インスタンスに制限します。 <i>vrf-name</i> 引数は、VRF の名前を指定します。
----------------------------	---

Command Default ストリッピングは無効です。完全なユーザ名が RADIUS サーバに送信されます。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines RADIUS サーバにユーザ名を転送する前に、ユーザ名からドメインをストリッピングするように NAS を設定するには、**radius-server domain-stripping** コマンドを使用します。完全なユーザ名が user1@cisco.com の場合、**radius-server domain-stripping** コマンドを有効にすると、ユーザ名の「user1」が RADIUS サーバに転送されます。

right-to-left キーワードを使用して、左から右ではなく、右から左へユーザ名のデリミタを解析するように指定します。これにより、デリミタの2つのインスタンスを含む文字列で、いずれのデリミタでもユーザ名をストリッピングできます。たとえば、ユーザ名が user@cisco.com@cisco.net の場合、サフィックスは次の2つの方向でストリッピングできます。デフォルトの方向 (左から右) では、ユーザ名の「user」が RADIUS サーバに転送されます。**right-to-left** キーワードを設定すると、ユーザ名の「user@cisco.com」が RADIUS サーバに転送されます。

プレフィックスのストリッピングを有効にし、プレフィックスデリミタとして認識される1つまたは複数の文字を指定するには、**prefix-delimiter** キーワードを使用します。最初に設定した解析される文字がプレフィックスデリミタとして使用され、そのデリミタの前の文字はすべてストリッピングされます。

サフィックスデリミタとして認識される1つまたは複数の文字を指定するには、**delimiter** キーワードを使用します。最初に設定した解析される文字がサフィックスのデリミタとして使用され、そのデリミタの後の文字はすべてストリッピングされます。

ユーザ名からストリッピングする特定のサフィックスを指定するには、**strip-suffix** *suffix* を使用します。たとえば、**radius-server domain-stripping strip-suffix cisco.net** コマンドを設定すると、username user@cisco.net がストリッピングされますが、username user@cisco.com はストリッピングされません。**radius-server domain-stripping** コマンドの複数のインスタンスを発行することによって、ストリッピング用に複数のサフィックスを設定できます。デフォルトのサフィックスデリミタは @ 文字です。



Note `radius-server domain-stripping s trip-suffix suffix` コマンドを発行すると、すべてのドメインからサフィックスをストリッピングする能力が無効になります。フルユーザ名からサフィックスが削除されるのは、サフィックス デリミタとサフィックスの両方が一致した場合のみです。 **delimiter** キーワードを使用して別のサフィックスデリミタまたは一連のサフィックスデリミタを指定しない場合は、デフォルトのサフィックスデリミタである `@` が使用されます。

指定した VRF のみにドメインストリッピング設定を適用するには、`vrf vrf-name` オプションを使用します。

次に、さまざまなタイプのドメインストリッピング設定間の連携動作を示します。

- `radius-server domain-stripping[right-to-left] [prefix-delimiter character [character2...character7]] [delimiter character [character2...character7]]` コマンドに設定できるインスタンスは1つのみです。
- `vrf vrf-name` に一意の値を使用した `radius-server domain-stripping[right-to-left] [prefix-delimiter character [character2...character7]] [delimiter character [character2...character7]] [vrf vrf-name]` コマンドは、複数のインスタンスを設定できます。
- `radius-server domain-stripping strip-suffix suffix[vrf per-vrf]` コマンドのインスタンスを複数設定することで、グローバルまたは VRF ごとのルールセットの一部として複数のサフィックスをストリッピングすることができます。
- 別のデリミタまたは一連のデリミタを指定した場合を除き、任意のバージョンの `radius-server domain-stripping` コマンドを発行すると、そのルールセットにデフォルトのデリミタ文字の `@` を使用するサフィックスストリッピングが自動的に有効になります。
- サフィックスごとのストリッピングルールを設定すると、そのルールセットの汎用サフィックスストリッピングが無効になります。設定された1つまたは複数のサフィックスと一致するサフィックスのみがユーザ名からストリッピングされます。

Examples

次の例では、ルータのユーザ名を右から左へ解析するように設定し、`@`、`\`、および `$` を有効なサフィックス デリミタ文字として設定します。完全なユーザ名が `cisco/user@cisco.com$cisco.net` の場合、ユーザ名を右から左へ解析するとき `$` 文字が NAS によって検出される最初の有効なデリミタであるため、ユーザ名の「`cisco/user@cisco.com`」が RADIUS サーバに転送されます。

```
radius-server domain-stripping right-to-left delimiter @\ $
```

次の例は、ルータが、`abc` と名付けられた VRF インスタンスに関連するユーザのみに対して、ユーザ名からドメイン名を削除する設定を示します。デフォルトのサフィックス デリミタである `@` は一般的なサフィックスの削除に使用されます。

```
radius-server domain-stripping vrf abc
```

次の例は、`/` をプレフィックスデリミタとして使用して、プレフィックスの削除を有効にします。デフォルトのサフィックス デリミタ文字の `@` が一般的なサフィックスの削除に

使用されます。完全なユーザ名が `cisco/user@cisco.com` の場合、ユーザ名の「user」が RADIUS サーバに転送されます。

```
radius-server domain-stripping prefix-delimiter /
```

次の例は、プレフィックスの削除を有効にし、/の文字をプレフィックスデリミタとして設定し、#をサフィックスのデリミタとして設定します。完全なユーザ名が `cisco/user@cisco.com#cisco.net` の場合、ユーザ名の「user@cisco.com」が RADIUS サーバに転送されます。

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

次の例は、プレフィックスの削除を有効にし、/の文字をプレフィックスデリミタとして設定し、\$、@、および#をサフィックスのデリミタとして設定し、`cisco.com` のサフィックスのサフィックスごとの削除を設定します。完全なユーザ名が `cisco/user@cisco.com` の場合、ユーザ名の「user」が RADIUS サーバに転送されます。フルユーザ名が `cisco/user@cisco.com#cisco.net` であればユーザ名の「user@cisco.com」が転送されます。

```
radius-server domain-stripping prefix-delimiter / delimiter $#  
radius-server domain-stripping strip-suffix cisco.com
```

次の例では、ルータのユーザ名を右から左へ解析するように設定し、`cisco.com` のサフィックスでユーザ名のサフィックス削除を有効にします。完全なユーザ名が `cisco/user@cisco.net@cisco.com` の場合、ユーザ名の「cisco/user@cisco.net」が RADIUS サーバに転送されます。フルユーザ名が `cisco/user@cisco.com@cisco.net` であれば、このフルユーザ名が転送されます。

```
radius-server domain-stripping right-to-left  
radius-server domain-stripping strip-suffix cisco.com
```

次の例は、@をデリミタとして使用して `cisco.com` のサフィックスを削除する一連のグローバルな削除ルールと、`myvrf` という名前の VRF と関連するユーザ名に対する異なった一連の削除ルールを設定します。

```
radius-server domain-stripping strip-suffix cisco.com  
!  
radius-server domain-stripping prefix-delimiter # vrf myvrf  
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
ip vrf	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
tacacs-server domain-stripping	ユーザ名を TACACS+ サーバに転送する前にユーザ名からプレフィックスまたはサフィックスをストリッピングするようにルータを設定します。

sak-rekey

定義された MKA ポリシーのセキュリティアソシエーションキー (SAK) のキー再生成間隔を設定するには、MKA ポリシーコンフィギュレーションモードで **sak-rekey** コマンドを使用します。SAK キー再生成タイマーを無効にするには、このコマンドの **no** 形式を使用します。

sak-rekey {*interval time-interval* | **on-live-peer-loss**}

no sak-rekey {*interval* | **on-live-peer-loss**}

Syntax Description

interval	SAK キー再生成間隔を秒単位で設定します。
<i>time-interval</i>	範囲は 30 ～ 65535 で、デフォルトは 0 です。
on-live-peer-loss	ライブメンバーシップからのピア損失。

Command Default

SAK キー再生成タイマーは無効になっています。デフォルトは 0 です。

Command Modes

MKA ポリシー コンフィギュレーション (config-mka-policy)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、SAK キー再生成間隔を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# sak-rekey interval 300
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
send-secure-announcements	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。

Command	Description
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

security level (IPv6 スヌーピング)

適用されるセキュリティのレベルを指定するには、IPv6 スヌーピングポリシーコンフィギュレーションモードで **security-level** コマンドを使用します。

security level {glean | guard | inspect}

Syntax Description		
glean	アドレスをメッセージから抽出し、検証を行わずにそれらをバインディングテーブルにインストールします。	
guard	収集と検査の両方を実行します。さらに、信頼できるポートで受信されていない場合、または別のポリシーによって許可されていない場合、RA メッセージおよび DHCP サーバメッセージは拒否されます。	
inspect	メッセージの一貫性と準拠度を検証します。特に、アドレス所有権が強制されます。無効なメッセージはドロップされます。	
Command Default	デフォルトのセキュリティ レベルは guard です。	
Command Modes	IPv6 スヌーピング コンフィギュレーション (config-ipv6-snooping)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、IPv6 スヌーピングポリシー名を **policy1** と定義し、セキュリティレベルを **inspect** として設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
Device(config-ipv6-snooping)# end
```

send-secure-announcements

MKA が MACsec Key Agreement Protocol Data Unit (MKPDU) でセキュアな通知を送信できるようにするには、MKA ポリシー コンフィギュレーションモードで **send-secure-announcements** コマンドを使用します。このセキュアな通知の送信を無効にするには、このコマンドの **no** 形式を使用します。

send-secure-announcements
no send-secure-announcements

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

MKPDU でのセキュアなアナウンスは無効になっています。

Command Modes

MKA ポリシー コンフィギュレーション (config-mka-policy)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

セキュアなアナウンスは、以前はセキュアでないアナウンスで共有されていた MACsec 暗号スイート機能を再検証します。

Examples

次に、セキュアなアナウンスの送信を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# send-secure-announcements
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。

Command	Description
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

server-private (RADIUS)

グループサーバに対して、プライベート RADIUS サーバの IP アドレスを設定するには、RADIUS サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。関連付けられたプライベートサーバを認証、許可、およびアカウントिंग (AAA) グループサーバから削除するには、このコマンドの **no** 形式を使用します。

server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

<i>ip-address</i>	プライベート RADIUS サーバホストの IP アドレス。
auth-port <i>port-number</i>	(任意) 認証要求に対するユーザ データグラム プロトコル (UDP) 宛先ポート。デフォルト値は 1645 です。
acct-port <i>port-number</i>	(任意) アカウントING要求に対する UDP 宛先ポート。デフォルト値は 1646 です。
non-standard	(任意) RADIUS サーバでベンダー独自の RADIUS 属性を使用。
timeout <i>seconds</i>	(オプション) デバイスが RADIUS サーバの応答を待機し、再送信するまでの時間間隔 (秒単位)。この設定は radius-server timeout コマンドのグローバル値を上書きします。タイムアウト値が指定されていない場合は、グローバル値が使用されます。
retransmit <i>retries</i>	(任意) サーバが応答しない、または応答が遅い場合に RADIUS 要求をサーバに再送信する回数。この設定は radius-server retransmit コマンドのグローバル設定を上書きします。
key <i>string</i>	(任意) デバイスと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キー。このキーは radius-server key コマンドのグローバル設定を上書きします。キー文字列を指定しない場合、グローバル値が使用されます。 <i>string</i> には、 0 (暗号化されていないキーが続くことを指定)、 6 (Advanced Encryption Scheme (AES) 暗号化キーが続くことを指定) 7 (非公開のキーが続くことを指定) または暗号化されていない (クリアテキスト) サーバキーを指定する行を指定できます。

Command Default

server-private パラメータが指定されていない場合は、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合は、デフォルト値が使用されます。

Command Modes

RADIUS サーバグループ コンフィギュレーション (config-sg-radius)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

server-private コマンドを使用して、特定のプライベートサーバと定義済みのサーバグループを関連付けます。Virtual Route Forwarding (VRF) インスタンス間でプライベートアドレスが重複する可能性を防ぐには、プライベートサーバ（プライベートアドレスを持つサーバ）をサーバグループ内で定義し、他のグループには示されないようにします。この場合も、グローバルプール（デフォルトの「radius」サーバグループなど）内のサーバは、IPアドレスとポート番号を使って参照できます。このように、サーバグループ内のサーバのリストには、グローバルコンフィギュレーションにおけるホストの参照情報とプライベートサーバの定義が含まれます。



Note

- **radius-server directed-request** コマンドが設定されている場合、**server-private (RADIUS)** コマンドを設定してプライベート RADIUS サーバをグループサーバとして使用することはできません。
- プライベート RADIUS サーバの AAA サーバ統計情報レコードの作成または更新はサポートされていません。プライベート RADIUS サーバが使用されている場合、エラーメッセージとトレースバックが発生しますが、これらのエラーメッセージやトレースバックは AAA RADIUS 機能には影響しません。これらのエラーメッセージとトレースバックを回避するには、プライベート RADIUS サーバの代わりにパブリック RADIUS サーバを設定します。

タイプ 6 AES 暗号化キーを設定するには、**password encryption aes** コマンドを使用します。

Examples

次に、sg_water RADIUS グループサーバを定義してプライベートサーバを関連付ける例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# end
```

Related Commands

コマンド	説明
aaa group server	各種のサーバホストを別個のリストと別個の方式にグループ化します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
password encryption aes	タイプ 6 の暗号化事前共有キーをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。

コマンド	説明
radius-server directed-request	ユーザが NAS にログインして認証用の RADIUS サーバを選択できるようにします。

server-private (TACACS+)

グループサーバに対してプライベート TACACS+ サーバの IPv4 アドレスまたは IPv6 アドレスを設定するには、**server-private** コマンドをサーバグループ コンフィギュレーション モードで使用します。関連付けられたプライベートサーバを認証、許可、およびアカウントिंग (AAA) グループサーバから削除するには、このコマンドの **no** 形式を使用します。

```
server-private { ipv4-address | ipv6-address | fqdn } [ nat ] [ single-connection ] [ port port-number ] [ timeout seconds ] key [ 0 | 7 ] string
no server-private
```

Syntax Description	
ipv4-address	プライベート TACACS+ サーバホストの IPv4 アドレスです。
ipv6-address	プライベート TACACS+ サーバホストの IPv6 アドレスです。
fqdn	ドメインネームサーバ (DNS) からのアドレス解決のためのプライベート TACACS+ サーバホストの完全修飾ドメイン名 (fqdn)。
nat	(任意) リモートデバイスのポートのネットワークアドレス変換 (NAT) アドレスを指定します。このアドレスは TACACS+ サーバに送信されます。
single-connection	(任意) ルータと TACACS+ サーバ間の単一の TCP 接続を維持します。
timeoutseconds	(任意) サーバ応答のタイムアウト値を指定します。この値を指定すると、このサーバに限り、 tacacs-server timeout コマンドで設定されたグローバルタイムアウト値が上書きされます。
portport-number	(任意) サーバのポート番号を指定します。この設定によって、デフォルトのポート 49 は上書きされます。
key [0 7] string	(任意) 認証と暗号キーを指定します。このキーは TACACS+ デーモンで使用されるキーと一致する必要があります。このキーを指定すると、このサーバに対してグローバル tacacs-server key コマンドで設定されたキーのみが上書きされます。 数字を入力しないか、または 0 を入力した場合は、入力された文字列はプレーンテキストと見なされます。7 を入力すると、入力された文字列は暗号化されたテキストと見なされます。

Command Default server-private パラメータが指定されていない場合は、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合は、デフォルト値が使用されます。

Command Modes TACACS+ サーバグループ コンフィギュレーション (config-sg-tacacs+)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

server-private コマンドを使用して、特定のプライベートサーバと定義済みのサーバグループを関連付けます。Virtual Route Forwarding (VRF) 間でプライベートアドレスが重複する可能性を防ぐには、プライベートサーバ (プライベートアドレスを持つサーバ) をサーバグループ内で定義し、他のグループには示されないようにします。この場合も、グローバルプール (デフォルトの「TACACS+」サーバグループ) 内のサーバは、IP アドレスとポート番号を使用して参照できます。このように、サーバグループ内のサーバのリストには、グローバルコンフィギュレーションにおけるホストの参照情報とプライベートサーバの定義が含まれます。

次に、tacacs1 TACACS+ グループサーバを定義してプライベートサーバを関連付ける例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco
Device(config-sg-tacacs+)# exit
Device(config)# ip vrf cisco
Device(config-vrf)# rd 100:1
Device(config-vrf)# exit
Device(config)# interface Loopback0
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# ip vrf forwarding cisco
```

Related Commands

コマンド	説明
aaa group server	各種のサーバホストを別個のリストと別個の方式にグループ化します。
aaa new-model	AAA アクセスコントロールモデルをイネーブルにします。
ip tacacs source-interface	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ip vrf forwarding (server-group)	AAA TACACS+ サーバグループの VRF の参照を設定します。

show aaa clients

認証、許可、およびアカウントティング（AAA）クライアントの統計情報を表示するには、**show aaa clients** コマンドを使用します。

show aaa clients [detailed]

Syntax Description	detailed （任意）詳細なAAAクライアントの統計情報を示します。
---------------------------	---

Command Modes	ユーザ EXEC (>) 特権 EXEC (#)
----------------------	-----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show aaa clients** コマンドの出力例を示します。

```
Device> enable
Device# show aaa clients

Dropped request packets: 0
```

show aaa command handler

認証、許可、およびアカウントティング（AAA）コマンドハンドラの統計情報を表示するには、**show aaa command handler** コマンドを使用します。

show aaa command handler

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show aaa command handler** コマンドの出力例を示します。

```
Device# show aaa command handler

AAA Command Handler Statistics:
  account-logon: 0, account-logout: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logout: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

show aaa dead-criteria

認証、許可、およびアカウンティング（AAA）の **dead-criteria** 検出情報を表示するには、**show aaa dead-criteria** コマンドを特権 EXEC モードで使用します。

```
show aaa dead-criteria {security-protocol ip-address} [auth-port port-number] [acct-port port-number][server-group-name]
```

Syntax Description

security-protocol	指定した AAA サーバのセキュリティプロトコル。現在、サポートされているプロトコルは RADIUS のみです。
<i>ip-address</i>	指定した AAA サーバの IP アドレス。
auth-port	（任意）指定した RADIUS サーバの認証ポート。
<i>port-number</i>	（任意）認証ポートの番号。デフォルトは 1645 です（RADIUS サーバの場合）。
acct-port	（任意）指定した RADIUS サーバのアカウンティングポート。
<i>port-number</i>	（任意）アカウンティングポートの番号。デフォルトは 1646 です（RADIUS サーバの場合）。
<i>server-group-name</i>	（任意）指定したサーバが関連付けられているサーバグループ。デフォルトは <i>radius</i> です（RADIUS サーバの場合）。

Command Default

現在、**auth-port** キーワードの *port-number* 引数と **acct-port** キーワードの *port-number* 引数は、デフォルトでそれぞれ 1645 と 1646 になります。*server-group-name* 引数のデフォルトは *radius* です。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

同じ IP アドレスを持つ複数の RADIUS サーバをデバイスに設定できます。**auth-port** キーワードと **acct-port** キーワードはサーバを区別するために使用されます。指定したサーバグループに関連付けられているサーバの **dead** 検出間隔は、**server-group-name** キーワードを使用して取得できません（RADIUS サーバの **dead** 状態検出間隔と再送信の値は、サーバが属するサーバグループに基づいて設定されます。複数のサーバグループに同じサーバを含めることができます）。

Examples

次に、IP アドレス 172.19.192.80 の RADIUS サーバに対して **dead-criteria** 検出情報を要求した場合の例を示します。

```
Device# show aaa dead-criteria radius 172.19.192.80 radius
```

```
RADIUS Server Dead Criteria:
```

```
=====
```

```
Server Details:
```

```
Address : 172.19.192.80
```

```
Auth Port : 1645
```

```
Acct Port : 1646
```

```
Server Group : radius
```

```
Dead Criteria Details:
```

```
Configured Retransmits : 62
```

```
Configured Timeout : 27
```

```
Estimated Outstanding Transactions: 5
```

```
Dead Detect Time : 25s
```

```
Computed Retransmit Tries: 22
```

```
Statistics Gathered Since Last Successful Transaction
```

```
=====
```

```
Max Computed Outstanding Transactions: 5
```

```
Max Computed Dead Detect Time: 25s
```

```
Max Computed Retransmits : 22
```

Max Computed Dead Detect Time が表示されます（秒単位）。表示される他のフィールドは説明がなくてもわかります。

Related Commands

コマンド	説明
debug aaa dead-criteria transactions	デッド条件の AAA トランザクションの値を表示します。
radius-server dead-criteria	RADIUS サーバをデッド状態と指定するための条件のいずれかまたは両方を、指定した定数で適用します。
show aaa server-private	すべてのプライベート RADIUS サーバのステータスを表示します。
show aaa servers	AAA サーバとの間で送受信されたパケットの数に関する情報を表示します。

show aaa local

認証、許可、およびアカウンティング（AAA）ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

show aaa local {**netuser** {*name* | **all**} | **statistics** | **user lockout**}

Syntax Description	
netuser	AAA ローカル ネットワークまたはゲストユーザデータベースを指定します。
<i>name</i>	ネットワーク ユーザ名。
all	ネットワークおよびゲスト ユーザ情報を指定します。
statistics	ローカル認証の統計情報を表示します。
user lockout	AAA ローカルのロックアウトされたユーザを指定します。

Command Modes	
	ユーザ EXEC (>)
	特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show aaa local statistics** コマンドの出力例を示します。

```
Device# show aaa local statistics

Local EAP statistics

EAP Method          Success          Fail
-----
Unknown              0                 0
EAP-MD5              0                 0
EAP-GTC              0                 0
LEAP                 0                 0
PEAP                 0                 0
EAP-TLS              0                 0
EAP-MSCHAPV2        0                 0
EAP-FAST             0                 0

Requests received from AAA:          0
Responses returned from EAP:        0
Requests dropped (no EAP AVP):      0
Requests dropped (other reasons):    0
Authentication timeouts from EAP:   0

Credential request statistics
Requests sent to backend:            0
```

```
Requests failed (unable to send):          0
Authorization results received

Success:                                   0
Fail:                                       0
```

show aaa servers

認証、許可、アカウントिंग（AAA）サーバの MIB によって認識されるすべての AAA サーバを表示するには、**show aaa servers** コマンドを使用します。

show aaa servers [private | public | [detailed]]

Syntax Description	detailed	(任意) AAA サーバの MIB によって認識されるプライベート AAA サーバを表示します。
	public	(任意) AAA サーバの MIB によって認識されるパブリック AAA サーバを表示します。
	detailed	(任意) 詳細な AAA サーバの統計情報を表示します。
Command Modes	ユーザ EXEC (>)	
	特権 EXEC (>)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**show aaa servers** コマンドの出力例を示します。

show aaa sessions

認証、許可、アカウントिंग（AAA）セッションの MIB によって認識される AAA セッションを表示するには、**show aaa sessions** コマンドを使用します。

show aaa sessions

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース

変更内容

Cisco IOS XE Fuji 16.9.2

このコマンドが導入されました。

次に、**show aaa sessions** コマンドの出力例を示します。

```
Device# show aaa sessions

Total sessions since last reload: 7
Session Id: 4007
  Unique Id: 4025
  User Name: *not available*
  IP Address: 0.0.0.0
  Idle Time: 0
  CT Call Handle: 0
```

show authentication brief

特定のインターフェイスの認証セッションに関する概要情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show authentication brief** コマンドを使用します。

```
show authentication brief [switch {switch-number | active | standby} {R0}]
```

Syntax Description		
<i>switch-number</i>	<i>switch-number</i> 変数の有効な値は 1 ~ 9 です。	
R0	ルートプロセッサ (RP) スロット 0 に関する情報を表示します。	
active	アクティブ インスタンスを指定します。	
standby	スタンバイ インスタンスを指定します。	
Command Modes	特権 EXEC (#) ユーザ EXEC (>)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief
```

Interface	MAC Address	AuthC	AuthZ	Fg	Uptime
Gi2/0/14	0002.0002.0001	m:NA d:OK	AZ: SA-	X	281s
Gi2/0/14	0002.0002.0002	m:NA d:OK	AZ: SA-	X	280s
Gi2/0/14	0002.0002.0003	m:NA d:OK	AZ: SA-	X	279s
Gi2/0/14	0002.0002.0004	m:NA d:OK	AZ: SA-	X	278s
Gi2/0/14	0002.0002.0005	m:NA d:OK	AZ: SA-	X	278s
Gi2/0/14	0002.0002.0006	m:NA d:OK	AZ: SA-	X	277s
Gi2/0/14	0002.0002.0007	m:NA d:OK	AZ: SA-	X	276s
Gi2/0/14	0002.0002.0008	m:NA d:OK	AZ: SA-	X	276s
Gi2/0/14	0002.0002.0009	m:NA d:OK	AZ: SA-	X	275s
Gi2/0/14	0002.0002.000a	m:NA d:OK	AZ: SA-	X	275s
Gi2/0/14	0002.0002.000b	m:NA d:OK	AZ: SA-	X	274s
Gi2/0/14	0002.0002.000c	m:NA d:OK	AZ: SA-	X	274s
Gi2/0/14	0002.0002.000d	m:NA d:OK	AZ: SA-	X	273s
Gi2/0/14	0002.0002.000e	m:NA d:OK	AZ: SA-	X	273s
Gi2/0/14	0002.0002.000f	m:NA d:OK	AZ: SA-	X	272s
Gi2/0/14	0002.0002.0010	m:NA d:OK	AZ: SA-	X	272s
Gi2/0/14	0002.0002.0011	m:NA d:OK	AZ: SA-	X	271s
Gi2/0/14	0002.0002.0012	m:NA d:OK	AZ: SA-	X	271s
Gi2/0/14	0002.0002.0013	m:NA d:OK	AZ: SA-	X	270s
Gi2/0/14	0002.0002.0014	m:NA d:OK	AZ: SA-	X	270s
Gi2/0/14	0002.0002.0015	m:NA d:OK	AZ: SA-	X	269s

次に、アクティブインスタンスに対する **show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief switch active R0
```

Interface	MAC Address	AuthC	AuthZ	Fg	Uptime
Gi2/0/14	0002.0002.0001	m:NA d:OK	AZ: SA-	X	1s
Gi2/0/14	0002.0002.0002	m:NA d:OK	AZ: SA-	X	0s
Gi2/0/14	0002.0002.0003	m:NA d:OK	AZ: SA-	X	299s
Gi2/0/14	0002.0002.0004	m:NA d:OK	AZ: SA-	X	298s
Gi2/0/14	0002.0002.0005	m:NA d:OK	AZ: SA-	X	298s
Gi2/0/14	0002.0002.0006	m:NA d:OK	AZ: SA-	X	297s
Gi2/0/14	0002.0002.0007	m:NA d:OK	AZ: SA-	X	296s
Gi2/0/14	0002.0002.0008	m:NA d:OK	AZ: SA-	X	296s
Gi2/0/14	0002.0002.0009	m:NA d:OK	AZ: SA-	X	295s
Gi2/0/14	0002.0002.000a	m:NA d:OK	AZ: SA-	X	295s
Gi2/0/14	0002.0002.000b	m:NA d:OK	AZ: SA-	X	294s
Gi2/0/14	0002.0002.000c	m:NA d:OK	AZ: SA-	X	294s
Gi2/0/14	0002.0002.000d	m:NA d:OK	AZ: SA-	X	293s
Gi2/0/14	0002.0002.000e	m:NA d:OK	AZ: SA-	X	293s
Gi2/0/14	0002.0002.000f	m:NA d:OK	AZ: SA-	X	292s
Gi2/0/14	0002.0002.0010	m:NA d:OK	AZ: SA-	X	292s
Gi2/0/14	0002.0002.0011	m:NA d:OK	AZ: SA-	X	291s
Gi2/0/14	0002.0002.0012	m:NA d:OK	AZ: SA-	X	291s
Gi2/0/14	0002.0002.0013	m:NA d:OK	AZ: SA-	X	290s
Gi2/0/14	0002.0002.0014	m:NA d:OK	AZ: SA-	X	290s
Gi2/0/14	0002.0002.0015	m:NA d:OK	AZ: SA-	X	289s
Gi2/0/14	0002.0002.0016	m:NA d:OK	AZ: SA-	X	289s

次に、スタンバイインスタンスに対する **show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief switch standby R0
```

```
No sessions currently exist
```

次の表で、この出力で表示される重要なフィールドについて説明します。

Table 148: show authentication brief フィールドの説明

フィールド	説明
Interface	認証インターフェイスのタイプと番号。
MAC アドレス	クライアントの MAC アドレス。
AuthC	認証ステータス。
authz	承認ステータス。

フィールド	説明
FG	<p>現在のステータスを示すフラグ。有効な値は次のとおりです。</p> <ul style="list-style-type: none">• A: ポリシーの適用中（詳細は複数行のステータスを参照）• D: 取り外し待ち• F: 最終の取り外しの進行中• I: IIF ID の割り当て待ち• P: セッションをプッシュ済み• R: ユーザプロファイルの削除中（詳細は複数行のステータスを参照）• U: ユーザプロファイルの適用中（詳細は複数行のステータスを参照）• X: 不明なブロック
Uptime	セッションが起動してからの経過時間。

show authentication sessions

現在の認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。

```
show authentication sessions [database] [handle handle-id [details]] [interface type number
[details] [mac mac-address [interface type number] [method method-name [interface type number
[details] [session-id session-id [details]]]
```

Syntax Description

database	(任意) セッションデータベースに格納されているデータだけを示します。
handle <i>handle-id</i>	(任意) 認証マネージャ情報を表示する特定のハンドルを指定します。
details	(任意) 詳細情報を表示します。
interface <i>type number</i>	(任意) 認証マネージャ情報を表示する特定のインターフェイスのタイプと番号を指定します。
mac <i>mac-address</i>	(任意) 情報を表示する特定の MAC アドレスを指定します。
method <i>method-name</i>	(任意) 認証マネージャ情報を表示する特定の認証方法を指定します。方法を指定する場合 (dot1x 、 mab 、または webauth)、インターフェイスも指定できます。
session-id <i>session-id</i>	(任意) 認証マネージャ情報を表示する特定のセッションを指定します。

Command Modes

ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

現在のすべての認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。特定の認証マネージャセッションに関する情報を表示するには、1 つ以上のキーワードを使用します。

このテーブルは、報告された認証セッションで想定される動作状態を示します。

Table 149: 認証方式の状態

状態	説明
Not run	このセッションの方式は実行されていません。
Running	このセッションの方式が実行中です。

状態	説明
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次の表に、使用できる認証方式を示します。

Table 150: 認証方式の状態

状態	説明
dot1x	802.1X
mab	MAC 認証バイパス
webauth	Web 認証

次に、デバイス上のすべての認証セッションを表示する例を示します。

Device# **show authentication sessions**

```

Interface      MAC Address      Method  Domain  Status      Session ID
Gi1/0/48      0015.63b0.f676  dot1x   DATA   Authz Success 0A3462B1000000102983C05C
Gi1/0/5       000f.23c4.a401  mab     DATA   Authz Success 0A3462B10000000D24F80B58
Gi1/0/5       0014.bf5d.d26d  dot1x   DATA   Authz Success 0A3462B10000000E29811B94

```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

Device# **show authentication sessions interface gigabitethernet2/0/47**

```

          Interface: GigabitEthernet2/0/47
          MAC Address: Unknown
          IP Address: Unknown
          Status: Authz Success
          Domain: DATA
          Oper host mode: multi-host
          Oper control dir: both
          Authorized By: Guest Vlan
          Vlan Policy: 20
          Session timeout: N/A
          Idle timeout: N/A
          Common Session ID: 0A3462C8000000000002763C
          Acct Session ID: 0x00000002
          Handle: 0x25000000
Runnable methods list:
          Method      State
          mab         Failed over
          dot1x       Failed over
-----

```

```
Interface: GigabitEthernet2/0/47
MAC Address: 0005.5e7c.da05
IP Address: Unknown
User-Name: 00055e7cda05
  Status: Authz Success
  Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
  Authorized By: Authentication Server
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462C8000000010002A238
Acct Session ID: 0x00000003
  Handle: 0x91000001
Runnable methods list:
Method      State
mab         Authc Success
dot1x      Not run
```

show cisp

指定されたインターフェイスの Client Information Signaling Protocol (CISP) 情報を表示するには、特権 EXEC モードで **show cisp** コマンドを使用します。

show cisp {[**clients** | **interface** *interface-id*] | **registrations** | **summary**}

Syntax Description		
clients		(任意) CISP クライアントの詳細を表示します。
interface <i>interface-id</i>		(任意) 指定されたインターフェイスの CISP 情報を表示し、クライアントとポートチャネルが含まれます。
registrations		CISP の登録情報を表示します。
summary		(任意) CISP のサマリー情報を表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show cisp interface** コマンドの出力例を示します。

```
Device# show cisp interface fastethernet 0/1/1
CISP not enabled on specified interface
```

次に、**show cisp registration** コマンドの出力例を示します。

```
Device# show cisp registrations
Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
```

Gi3/0/3
Gi3/0/5
Gi3/0/23

Related Commands

コマンド	説明
cisp enable	CISP をイネーブルにします。
dot1x credentials <i>profile</i>	プロファイルをサブリカントデバイスに設定

show dot1x

デバイスまたは指定されたポートの IEEE 802.1X 統計情報、管理ステータス、および動作ステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show dot1x** コマンドを使用します。

show dot1x [**all** [**count** | **details** | **statistics** | **summary**]] [**interface type number** [**details** | **statistics**]] [**statistics**]

Syntax Description	all	(任意) すべてのインターフェイスの IEEE 802.1X 情報を表示します。
	count	(任意) 許可されたクライアントと無許可のクライアントの総数を表示します。
	details	(任意) IEEE 802.1X インターフェイスの詳細を表示します。
	statistics	(任意) すべてのインターフェイスの IEEE 802.1X 統計情報を表示します。
	summary	(任意) すべてのインターフェイスの IEEE 802.1X サマリー情報を表示します。
	interface type number	(任意) 指定したポートの IEEE 802.1X ステータスを表示します。

Command Modes	ユーザ EXEC (>) 特権 EXEC (#)
---------------	-----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show dot1x all** コマンドの出力例を示します。

```
Device# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

次に、**show dot1x all count** コマンドの出力例を示します。

```
Device# show dot1x all count
```

```
Number of Dot1x sessions
-----
Authorized Clients      = 0
Unauthorized Clients    = 0
Total No of Client      = 0
```

次に、**show dot1x all statistics** コマンドの出力例を示します。

```
Device# show dot1x statistics

Dot1x Global Statistics for
-----
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0
RxReq = 0        RxInvalid = 0    RxLenErr = 0
RxTotal = 0

TxStart = 0      TxLogoff = 0      TxResp = 0
TxReq = 0        ReTxReq = 0       ReTxReqFail = 0
TxReqID = 0      ReTxReqID = 0    ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

拡張可能認証プロトコル（EAP）のセキュアトンネリングを介したフレキシブル認証（FAST）ピアの格納済み Protected Access Credential（PAC）を表示するには、特権 EXEC モードで **show eap pac peer** コマンドを使用します。

show eap pac peer

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC（#）

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、**show eap pac peers** コマンドの出力例を示します。

```
Device# show eap pac peers
No PACs stored
```

Related Commands

コマンド	説明
clear eap sessions	デバイスまたは指定されたポートのEAPのセッションをクリアします。

show ip access-lists

現在のすべての IP アクセスリストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip access-lists** コマンドを使用します。

show ip access-lists [*access-list-number access-list-number-expanded-range access-list-name* | **dynamic** [*dynamic-access-list-name*] | **interface** *name number* [**in** | **out**]]

Syntax Description		
<i>access-list-number</i>	(任意)	表示する IP アクセス リストの数です。
<i>access-list-number-expanded-range</i>	(任意)	表示する IP アクセスリストの拡張範囲です。
<i>access-list-name</i>	(任意)	表示する IP アクセス リストの名前です。
dynamic <i>dynamic-access-list-name</i>	(任意)	指定されたダイナミック IP アクセスリストを表示します。
interface <i>name number</i>	(任意)	指定されたインターフェイスのアクセスリストを表示します。
in	(任意)	インターフェイスの入力統計情報を表示します。
out	(任意)	インターフェイスの出力統計情報を表示します。



Note OGACL の統計情報はサポートされていません

Command Default 標準の IP アクセスリストおよび拡張 IP アクセスリストがすべて表示されます。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **show ip access-lists** コマンドの出力は、IP 固有のもの以外は **show access-lists** コマンドの出力と同じです。また、特定のアクセスリストを指定できます。

show ip access-lists interface コマンドの出力には、dACL フィルタ ID や ACL フィルタ ID は表示されません。これは、物理インターフェイスではなく、各認証セッションのマルチドメイン認証によって作成された仮想ポートに ACL が接続されるためです。dACL フィルタ ID や ACL フィルタ ID を表示するには、**show ip access-lists access-list-name** コマンドを使用します。*access-list-name*

は、**show access-session interface interface-name detail** コマンドの出力から取得する必要があります。*access-list-name* では大文字と小文字が区別されます。

Examples

次に、すべてのアクセスリストを要求した場合の **show ip access-lists** コマンドの出力例を示します。

```
Device# show ip access-lists

Extended IP access list 101
  deny udp any any eq nntp
  permit tcp any any
  permit udp any any eq tftp
  permit icmp any any
  permit udp any any eq domain
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 151: show ip access-lists フィールドの説明

フィールド	説明
Extended IP access list	拡張 IP アクセス リスト名/番号。
deny	拒否するパケット。
udp	ユーザ データグラム プロトコル。
any	送信元ホストまたは宛先ホスト。
eq	特定のポート番号のパケット。
nntp	ネットワーク ニュース トランスポート プロトコル。
permit	転送するパケット。
tcp	伝送制御プロトコル。
tftp	Trivial File Transfer Protocol。
icmp	Internet Control Message Protocol (インターネット制御メッセージプロトコル)。
ドメイン	ドメインネームサービス。

次に、特定のアクセスリストの名前を要求した場合の **show ip access-lists** コマンドの出力例を示します。

```
Device# show ip access-lists Internetfilter

Extended IP access list Internetfilter
  permit tcp any 192.0.2.0 255.255.255.255 eq telnet
  deny tcp any any
  deny udp any 192.0.2.0 255.255.255.255 lt 1024
```

```
deny ip any any log
```

次に、**show ip access-lists** コマンドで **dynamic** キーワードを使用した場合の出力例を示します。

```
Device# show ip access-lists dynamic CM_SF#1

Extended IP access list CM_SF#1
 10 permit udp any any eq 5060 (650 matches)
 20 permit tcp any any eq 5060
 30 permit udp any any dscp ef (806184 matches)
```

Related Commands

Command	Description
deny	パケットを拒否する名前付き IP アクセス リストまたは OGACL の条件を設定します。
ip access-group	ACL または OGACL をインターフェイスまたはサービスポリシーマップに適用します。
ip access-list	IP アクセス リストまたは OGACL を名前または番号で定義します。
object-group network	OGACL で使用するネットワーク オブジェクト グループを定義します。
object-group service	OGACL で使用するサービス オブジェクト グループを定義します。
permit	パケットを許可する名前付き IP アクセスリストまたは OGACL の条件を設定します。
show object-group	設定されているオブジェクトグループに関する情報を表示します。
show run interfaces cable	ケーブルモデムの統計情報を表示します。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報を概要形式または詳細形式で表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp snooping statistics [detail]

Syntax Description **detail** (任意) 詳細な統計情報を表示します。

Command Modes ユーザ EXEC (>)
 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デバイスタックでは、すべての統計情報がスタックのアクティブスイッチで生成されます。新しいアクティブデバイスが選出された場合、統計カウンタはリセットされます。

次に、**show ip dhcp snooping statistics** コマンドの出力例を示します。

```
Device> show ip dhcp snooping statistics

Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

次に、**show ip dhcp snooping statistics detail** コマンドの出力例を示します。

```
Device> show ip dhcp snooping statistics detail

Packets Processed by DHCP Snooping                = 0
Packets Dropped Because
  IDB not known                                    = 0
  Queue full                                       = 0
  Interface is in errdisabled                      = 0
  Rate limit exceeded                             = 0
  Received on untrusted ports                     = 0
  Nonzero giaddr                                   = 0
  Source mac not equal to chaddr                  = 0
  Binding mismatch                                 = 0
  Insertion of opt82 fail                          = 0
  Interface Down                                  = 0
  Unknown output interface                        = 0
  Reply output port equal to input port           = 0
  Packet denied by platform                       = 0
```

次の表に、DHCP スヌーピング統計情報およびその説明を示します。

Table 152: DHCP スヌーピング統計情報

DHCP スヌーピング統計情報	説明
Packets Processed by DHCP Snooping	転送されたパケットおよびドロップされたパケットも含めて、DHCP スヌーピングによって処理されたパケットの合計数。
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートで DHCP パケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisable としてマークされたポートでパケットを受信した回数。これが発生する可能性があるのは、ポートが errdisable ステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバパケット (OFFER、ACK、NAK、LEASEQUERY のいずれか) を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレーエージェントアドレスフィールド (giaddr) がゼロ以外だった回数。または no ip dhcp snooping information option allow-untrusted グローバルコンフィギュレーションコマンドを設定しておらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレスフィールド (chaddr) がパケットの送信元 MAC アドレスと一致せず、 ip dhcp snooping verify mac-address グローバルコンフィギュレーションコマンドが設定されている回数。

DHCP スヌーピング統計情報	説明
Binding mismatch	MAC アドレスと VLAN のペアのバインディングになっているポートとは異なるポートで、RELEASE パケットまたは DECLINE パケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがデバイスの別のポートに移動して RELEASE または DECLINE を実行したことを表すこともあります。MAC アドレスは、イーサネットヘッダーの送信元 MAC アドレスではなく、DHCP パケットの chaddr フィールドから採用されます。
Insertion of opt82 fail	パケットへのオプション 82 挿入がエラーになった回数。オプション 82 データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。
Interface Down	パケットが DHCP リレー エージェントへの応答であるが、リレー エージェントの SVI インターフェイスがダウンしている回数。DHCP サーバへのクライアント要求の送信と応答の受信の間で SVI がダウンした場合に発生するエラーですが、めったに発生しません。
Unknown output interface	オプション 82 データまたは MAC アドレス テーブルのルックアップのいずれかで、DHCP 応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。オプション 82 が使用されておらず、クライアント MAC アドレスが期限切れになった場合に発生することがあります。ポートセキュリティ オプションで IPSG がイネーブルであり、オプション 82 がイネーブルでない場合、クライアントの MAC アドレスは学習されず、応答パケットはドロップされます。
Reply output port equal to input port	DHCP 応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。
Packet denied by platform	プラットフォーム固有のレジストリによってパケットが拒否された回数。

show platform software dns-umbrella statistics

デバイスのドメインネームシステム（DNS）の Umbrella の統計を表示するには、特権 EXEC モードで **show platform software dns-umbrella statistics** コマンドを使用します。

show platform software dns-umbrella statistics

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC (>)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、**show platform software dns-umbrella statistics** コマンドの出力例を示します。

```
Device> enable
Device# show platform software dns-umbrella statistics

=====
Umbrella Statistics
=====
Total Packets : 7848
DNSCrypt queries : 3940
DNSCrypt responses : 0
DNS queries : 0
DNS bypassed queries(Regex) : 0
DNS responses(Umbrella) : 0
DNS responses(Other) : 3906
Aged queries : 34
Dropped pkts : 0
```

show platform software umbrella switch F0

Embedded Service Processor (ESP) スロット 0 の Umbrella の設定を表示するには、特権 EXEC モードで **show platform software umbrella switch** *{switch_number | active | standby}* **F0** コマンドを使用します。

show platform software umbrella switch *{switch_number | active | standby}* **F0** *{config | interface-info | local-domain}*

Syntax Description	
switch <i>{switch_number active standby}</i>	スイッチを指定します。 <ul style="list-style-type: none"> • switch_number: スwitchの ID。有効な範囲は1～8です。 • active: アクティブスイッチを指定します。 • standby: スタンバイスイッチを指定します。
config	ESP スロット 0 のグローバル設定を表示します。
interface-info	ESP スロット 0 のインターフェイス関連の設定を表示します。
local-domain	ESP スロット 0 のローカルドメイン関連の設定を表示します。

Command Modes 特権 EXEC (>)

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、**show platform software umbrella switch active F0 config** コマンドの出力例を示します。

```
Device> show platform software umbrella switch active F0 config

+++ Umbrella Config +++

Umbrella feature:
-----
Init: Enabled
Dnscrypt: disabled

Timeout:
-----
udp timeout: 5

OrgId :
-----
orgid : 2427270
```

Resolver config:

RESOLVER IP's

208.67.220.220
208.67.222.222
2620:119:35::35
2620:119:53::53

Dnscrypt Info:

public_key:
magic_key:
serial number:

ProfileID	DeviceID	Mode	Resolver	Local-Domain	Tag

show radius server-group

RADIUS サーバグループのプロパティを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show radius server-group** コマンドを使用します。

show radius server-group {*name* | **all**}

Syntax Description *name* サーバグループの名前。サーバグループの名前の指定に使用する文字列は、**the aaa group server radius** コマンドを使用して定義する必要があります。

all すべてのサーバグループのプロパティを表示します。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **aaa group server radius** コマンドで定義したサーバグループを表示するには、**show radius server-group** コマンドを使用します。

次に、**show radius server-group all** コマンドの出力例を示します。

```
Device# show radius server-group all

Server group radius
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard Memlocks = 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 153: show radius server-groups コマンドのフィールドの説明

フィールド	説明
Server group	サーバグループの名前。
Sharecount	このサーバグループを共有している方式リストの数。たとえば、1つの方式リストが特定のサーバグループを使用する場合、sharecount は 1 です。2つの方式リストが同じサーバグループを使用する場合、sharecount は 2 です。
sg_unconfigured	サーバグループが設定解除されました。

フィールド	説明
Type	タイプは、standard または nonstandard のいずれかです。タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。
Memlocks	メモリ内にあるサーバグループ構造の内部参照の数。この数は、このサーバグループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。 Memlocks はメモリ管理のために内部的に使用されます。

show tech-support acl

テクニカルサポートに使用するアクセスコントロールリスト（ACL）関連の情報を表示するには、特権 EXEC モードで **show tech-support acl** コマンドを使用します。

show tech-support acl

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	

Usage Guidelines

show tech-support acl コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support acl | redirect flash:show_tech_acl.txt**）。

このコマンドの出力には次のコマンドが表示されます。



Note スタック可能なプラットフォームでは、これらのコマンドはスタック内のすべてのスイッチで実行されます。Catalyst 9400 シリーズ スイッチなどのモジュール型のプラットフォームでは、これらのコマンドはアクティブスイッチでのみ実行されます。



Note 次のコマンドのリストは、出力で使用可能なコマンドの例です。これらはプラットフォームによって異なる場合があります。

- **show clock**
- **show version**
- **show running-config**
- **show module**
- **show interface**
- **show access-lists**
- **show logging**
- **show platform software fed switch *switch-number* acl counters hardware**
- **show platform software fed switch *switch-number* ifm mapping**

- **show platform hardware fed switch *switch-number* fwd-asic drops exceptions**
- **show platform software fed switch *switch-number* acl info**
- **show platform software fed switch *switch-number* acl**
- **show platform software fed switch *switch-number* acl usage**
- **show platform software fed switch *switch-number* acl policy intftype all cam**
- **show platform software fed switch *switch-number* acl cam brief**
- **show platform software fed switch *switch-number* acl policy intftype all vcu**
- **show platform hardware fed switch *switch-number* acl resource usage**
- **show platform hardware fed switch *switch-number* fwd-asic resource tcam table acl**
- **show platform hardware fed switch *switch-number* fwd-asic resource tcam utilization**
- **show platform software fed switch *switch-number* acl counters hardware**
- **show platform software classification switch *switch-number* all F0 class-group-manager class-group**
- **show platform software process database forwarding-manager switch *switch-number* R0 summary**
- **show platform software process database forwarding-manager switch *switch-number* F0 summary**
- **show platform software object-manager switch *switch-number* F0 pending-ack-update**
- **show platform software object-manager switch *switch-number* F0 pending-issue-update**
- **show platform software object-manager switch *switch-number* F0 error-object**
- **show platform software peer forwarding-manager switch *switch-number* F0**
- **show platform software access-list switch *switch-number* f0 statistics**
- **show platform software access-list switch *switch-number* r0 statistics**
- **show platform software trace message fed switch *switch-number***
- **show platform software trace message forwarding-manager switch *switch-number* F0**
- **show platform software trace message forwarding-manager switch R0 *switch-number* R0**

Examples

次に、**show tech-support acl** コマンドの出力例を示します。

```
Device# show tech-support acl
.
.
.
----- show platform software fed switch 1 acl cam brief -----

Printing entries for region ACL_CONTROL (143) type 6 asic 0
=====
TAQ-4 Index-0 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Output IPv4 VACL

VCU Result: Not In-Use
```

```
L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

Source Address/Mask
0.0.0.0/0.0.0.0
Destination Address/Mask
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask   L4 Destination Port/Mask
0x0044 (68)/0xffff    0x0043 (67)/0xffff

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Forward L3, Forward L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

-----
TAQ-4 Index-1 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 VACL

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

Source Address/Mask
0.0.0.0/0.0.0.0
Destination Address/Mask
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask   L4 Destination Port/Mask
0x0043 (67)/0xffff    0x0044 (68)/0xffff

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Forward L3, Forward L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

-----
TAQ-4 Index-2 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 VACL

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

Source Address/Mask
0.0.0.0/0.0.0.0
Destination Address/Mask
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask   L4 Destination Port/Mask
0x0043 (67)/0xffff    0x0043 (67)/0xffff

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Forward L3, Forward L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

-----
```

```
TAQ-4 Index-3 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input IPv4 PACL

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

Source Address/Mask
0.0.0.0/0.0.0.0
Destination Address/Mask
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask    L4 Destination Port/Mask
0x0000 (0)/0x0000     0x0000 (0)/0x0000

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

-----
TAQ-4 Index-4 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 PACL

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

Source Address/Mask
0.0.0.0/0.0.0.0
Destination Address/Mask
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask    L4 Destination Port/Mask
0x0000 (0)/0x0000     0x0000 (0)/0x0000

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

-----
TAQ-4 Index-5 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output MAC PACL

VLAN ID/MASK : 0x000 (000)/0x000

Source MAC/Mask : 0000.0000.0000/0000.0000.0000

Destination MAC/Mask : 0000.0000.0000/0000.0000.0000

isSnap: Disabled, isLLC: Disabled

ACTIONS: Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

.
.
.
```

出力フィールドの意味は自明です。

show tech-support identity

テクニカルサポートに使用するアイデンティティ/802.1X 関連の情報を表示するには、特権 EXEC モードで **show tech-support identity** コマンドを使用します。

show tech-support identity mac *mac-address* interface *interface-name*

Syntax Description	mac <i>mac-address</i>	クライアント MAC アドレスに関する情報を表示します。
	interface <i>interface-name</i>	クライアント インターフェイスに関する情報を表示します。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
	Cisco IOS XE Gibraltar 16.11.1	

Usage Guidelines **show tech-support platform** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support identity mac *mac-address* interface *interface-name* | redirect flash:filename**）。

このコマンドの出力には次のコマンドが表示されます。

- **show clock**
- **show module**
- **show version**
- **show switch**
- **show redundancy**
- **show dot1x statistics**
- **show ip access-lists**
- **show interface**
- **show ip interface brief**
- **show vlan brief**
- **show running-config**
- **show logging**
- **show interface controller**

- show platform authentication sbinfo interface
- show platform host-access-table
- show platform pm port-data
- show spanning-tree interface
- show access-session mac detail
- show platform authentication session mac
- show device-tracking database mac details
- show mac address-table address
- show access-session event-logging mac
- show authentication sessions mac details R0
- show ip admission cache R0
- show platform software wired-client R0
- show platform software wired-client F0
- show platform software process database forwarding-manager R0 summary
- show platform software process database forwarding-manager F0 summary
- show platform software object-manager F0 pending-ack-update
- show platform software object-manager F0 pending-issue-update
- show platform software object-manager F0 error-object
- show platform software peer forwarding-manager R0
- show platform software peer forwarding-manager F0
- show platform software VP R0 summary
- show platform software VP F0 summary
- show platform software fed punt cpuq
- show platform software fed punt cause summary
- show platform software fed inject cause summary
- show platform hardware fed fwd-asic drops exceptions
- show platform hardware fed fwd-asic resource tcam table acl
- show platform software fed acl counter hardware
- show platform software fed matm macTable
- show platform software fed ifm mappings
- show platform software trace message fed reverse
- show platform software trace message forwarding-manager R0 reverse

- show platform software trace message forwarding-manager F0 reverse
- show platform software trace message smd R0 reverse
- show authentication sessions mac details
- show platform software wired-client
- show platform software process database forwarding-manager summary
- show platform software object-manager pending-ack-update
- show platform software object-manager pending-issue-update
- show platform software object-manager error-object
- show platform software peer forwarding-manager
- show platform software VP summary
- show platform software trace message forwarding-manager reverse
- show ip admission cache
- show platform software trace message smd reverse
- show platform software fed punt cpuq
- show platform software fed punt cause summary
- show platform software fed inject cause summary
- show platform hardware fed fwd-asic drops exceptions
- show platform hardware fed fwd-asic resource tcam table acl
- show platform software fed acl counter hardware
- show platform software fed matm macTable
- show platform software fed ifm mappings
- show platform software trace message fed reverse

Examples

次に、**show tech-support identity** コマンドの出力例を示します。

```
Device# show tech-support identity mac 0000.0001.0003 interface gigabitethernet1/0/1
.
.
.
----- show platform software peer forwarding-manager R0 -----
IOSD Connection Information:

MQIPC (reader) Connection State: Connected, Read-selected
Connections: 1, Failures: 22
3897 packet received (0 dropped), 466929 bytes
Read attempts: 2352, Yields: 0
BIPC Connection state: Connected, Ready
Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
36 packets sent, 2808 bytes
```

```
SMD Connection Information:

MQIPC (reader) Connection State: Connected, Read-selected
Connections: 1, Failures: 30
0 packet received (0 dropped), 0 bytes
Read attempts: 1, Yields: 0
MQIPC (writer) Connection State: Connected, Ready
Connections: 1, Failures: 0, Backpressures: 0
0 packet sent, 0 bytes

FP Peers Information:

Slot: 0
Peer state: connected
OM ID: 0, Download attempts: 638
Complete: 638, Yields: 0, Spurious: 0
IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
Back-Pressure asserted for IPC: 0, IPC-Log: 1
Number of FP FMAN peer connection expected: 7
Number of FP FMAN online msg received: 1
IPC state: unknown

Config IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
Tx Packets: 688, Messages: 2392, ACKs: 36
Rx Packets: 37, Bytes: 2068

IPC Log:
Peer name: fman-log-bay0-peer0
Flags: Recovery-Complete
Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 37, Bytes: 2864
Rx ACK Requests: 1, Tx ACK Responses: 1

Upstream FMRP-SMD IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
State: Connected
BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
State: Connected
BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
```

```
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
  State: Connected
  BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  OM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown

Config IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
  Tx Packets: 20, Messages: 704, ACKs: 1
  Rx Packets: 2, Bytes: 108

IPC Log:
  Peer name: fman-log-bay0-peer1
  Flags: Recovery-Complete
  Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-SMD IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
  State: Connected
  BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
  State: Connected
  BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
```

Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
 State: Connected
 BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
 TX Packets: 0, Bytes: 0, Drops: 0
 Rx Packets: 0, Bytes: 0
 Rx ACK Requests: 0, Tx ACK Responses: 0

----- show platform software peer forwarding-manager R0 -----

IOSD Connection Information:

MQIPC (reader) Connection State: Connected, Read-selected
 Connections: 1, Failures: 22
 3897 packet received (0 dropped), 466929 bytes
 Read attempts: 2352, Yields: 0
 BIPC Connection state: Connected, Ready
 Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
 36 packets sent, 2808 bytes

SMD Connection Information:

MQIPC (reader) Connection State: Connected, Read-selected
 Connections: 1, Failures: 30
 0 packet received (0 dropped), 0 bytes
 Read attempts: 1, Yields: 0
 MQIPC (writer) Connection State: Connected, Ready
 Connections: 1, Failures: 0, Backpressures: 0
 0 packet sent, 0 bytes

FP Peers Information:

Slot: 0
 Peer state: connected
 OM ID: 0, Download attempts: 638
 Complete: 638, Yields: 0, Spurious: 0
 IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
 Back-Pressure asserted for IPC: 0, IPC-Log: 1
 Number of FP FMAN peer connection expected: 7
 Number of FP FMAN online msg received: 1
 IPC state: unknown

Config IPC Context:

State: Connected, Read-selected
 BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
 Tx Packets: 688, Messages: 2392, ACKs: 36
 Rx Packets: 37, Bytes: 2068

IPC Log:

Peer name: fman-log-bay0-peer0
 Flags: Recovery-Complete
 Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:

State: Connected, Read-selected
 BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
 TX Packets: 0, Bytes: 0, Drops: 0
 Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:

```
State: Connected, Read-selected
BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 37, Bytes: 2864
Rx ACK Requests: 1, Tx ACK Responses: 1

Upstream FMRP-SMD IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
State: Connected
BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
State: Connected
BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
State: Connected
BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
OM ID: 1, Download attempts: 1
Complete: 1, Yields: 0, Spurious: 0
IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
Back-Pressure asserted for IPC: 0, IPC-Log: 0
Number of FP FMAN peer connection expected: 7
Number of FP FMAN online msg received: 1
IPC state: unknown

Config IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
Tx Packets: 20, Messages: 704, ACKs: 1
Rx Packets: 2, Bytes: 108

IPC Log:
Peer name: fman-log-bay0-peer1
Flags: Recovery-Complete
Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
```

```

TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

```

Upstream FMRP-SMD IPC Context:

```

State: Connected, Read-selected
BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

```

Upstream FMRP-WNCD_0 IPC Context:

```

State: Connected
BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

```

Upstream FMRP-WNCMGRD IPC Context:

```

State: Connected
BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

```

Upstream FMRP-MOBILITYD IPC Context:

```

State: Connected
BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

```

```
----- show platform software VP R0 summary -----
```

Forwarding Manager Vlan Port Information

Vlan	Intf-ID	Stp-state
1	7	Forwarding
1	9	Forwarding
1	17	Forwarding
1	27	Forwarding
1	28	Forwarding
1	29	Forwarding
1	30	Forwarding
1	31	Forwarding
1	40	Forwarding
1	41	Forwarding

Forwarding Manager Vlan Port Information

Vlan	Intf-ID	Stp-state
1	49	Forwarding
1	51	Forwarding
1	63	Forwarding
1	72	Forwarding
1	73	Forwarding
1	74	Forwarding

```
----- show platform software VP R0 summary -----
```

```
Forwarding Manager Vlan Port Information
```

Vlan	Intf-ID	Stp-state
1	7	Forwarding
1	9	Forwarding
1	17	Forwarding
1	27	Forwarding
1	28	Forwarding
1	29	Forwarding
1	30	Forwarding
1	31	Forwarding
1	40	Forwarding
1	41	Forwarding

```
Forwarding Manager Vlan Port Information
```

Vlan	Intf-ID	Stp-state
1	49	Forwarding
1	51	Forwarding
1	63	Forwarding
1	72	Forwarding
1	73	Forwarding
1	74	Forwarding

```
.  
. .  
. .
```

show umbrella

Cisco Umbrella 統合機能に関連する設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show umbrella** コマンドを使用します。

show umbrella {**config** | **deviceid** [**detailed**] | **dnscrypt**}

Syntax Description

config デバイスのグローバル設定を表示します。

deviceid デバイス登録の詳細を表示します。

dnscrypt DNSCrypt 関連の設定を表示します。

Command Modes

ユーザ EXEC (>)

特権 EXEC (>)

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Examples

次に、**show umbrella config** コマンドの出力例を示します。

```
Device> show umbrella config
```

```
Umbrella Configuration
=====
Token: 0C6ED7E376DD4D2E04492CE7EDFF1A7C00250986
API-KEY: NONE
OrganizationID: 2427270
Local Domain Regex parameter-map name: NONE
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

UDP Timeout: 5 seconds
Resolver address:
 1. 208.67.220.220
 2. 208.67.222.222
 3. 2620:119:53::53
 4. 2620:119:35::35
Umbrella Interface Config:
Number of interfaces with "umbrella out" config: 1
 1. GigabitEthernet1/0/48
    Mode      : OUT
    VRF       : global(Id: 0)
Number of interfaces with "umbrella in" config: 1
 1. GigabitEthernet1/0/1
    Mode      : IN
    DCA       : Disabled
    Tag       : test
    Device-id : 010a2c41b8ab019c
    VRF       : global(Id: 0)
```

```
Configured Umbrella Parameter-maps:  
  1. global
```

次に、**show umbrella deviceid detailed** コマンドの出力例を示します。

```
Device> show umbrella deviceid detailed  
  
Device registration details  
  1.GigabitEthernet1/0/2  
    Tag           : guest  
    Device-id     : 010a6aef0b443f0f  
    Description   : Device Id received successfully  
    WAN interface : GigabitEthernet1/0/1  
    WAN VRF used  : global(Id: 0)
```

次に、**show umbrella dnscrypt** コマンドの出力例を示します。

```
Device> show umbrella dnscrypt  
  
DNSEncrypt: Enabled  
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8DOC:BE04:BFAB:CA43:FB79  
Certificate Update Status:  
Last Successful Attempt : 10:55:40 UTC Apr 14 2016  
Last Failed Attempt : 10:55:10 UTC Apr 14 2016  
Certificate Details:  
Certificate Magic : DNSEncrypt  
Major Version : 0x0001  
Minor Version : 0x0000  
Query Magic : 0x717744506545635A  
Serial Number : 1435874751  
Start Time : 1435874751 (22:05:51 UTC Jul 2 2015)  
End Time : 1467410751 (22:05:51 UTC Jul 1 2016)  
Server Public Key :  
ABA1:F000:D394:8045:672D:73E0:EAE6:F181:19D0:2A62:3791:EFAD:B04E:40B7:B6F9:C40B  
Client Secret Key Hash :  
BBC3:409F:5CB5:C3F3:06BD:A385:78DA:4CED:62BC:3985:1C41:BCCE:1342:DF13:B71E:F4CF  
Client Public key :  
ECE2:8295:2157:6797:6BE2:C563:A5A9:C5FC:C20D:ADAF:EB3C:A1A2:C09A:40AD:CAEA:FF76  
NM key Hash :  
F9C2:2C2C:330A:1972:D484:4DD8:8E5C:71FF:6775:53A7:0344:5484:B78D:01B1:B938:E884
```

show vlan access-map

特定の VLAN アクセス マップまたはすべての VLAN アクセス マップに関する情報を表示するには、特権 EXEC モードで **show vlan access-map** コマンドを使用します。

show vlan access-map [*map-name*]

Syntax Description	<i>map-name</i> (任意) 特定の VLAN アクセスマップ名。
---------------------------	---

Command Modes	特権 EXEC (#)
----------------------	-------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、**show vlan access-map** コマンドの出力例を示します。

```
Device# show vlan access-map

Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward
```

show vlan filter

すべての VLAN フィルタ、または特定の VLAN または VLAN アクセス マップに関する情報を表示するには、特権 EXEC モードで **show vlan filter** コマンドを使用します。

```
show vlan filter {access-map name | vlan vlan-id}
```

Syntax Description	access-map <i>name</i> (任意) 指定された VLAN アクセス マップのフィルタリング情報を表示します。				
	vlan <i>vlan-id</i> (任意) 指定された VLAN のフィルタリング情報を表示します。指定できる範囲は 1 ~ 4094 です。				
Command Modes	特権 EXEC (#)				
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Fuji 16.9.2</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Examples

次に、**show vlan filter** コマンドの出力例を示します。

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

show vlan group

VLAN グループにマッピングされている VLAN を表示するには、特権 EXEC モードで **show vlan group** コマンドを使用します。

```
show vlan group [group-name vlan-group-name [user_count]]
```

Syntax Description	group-name <i>vlan-group-name</i> (任意) 指定した VLAN グループにマッピングされている VLAN を表示します。
	user_count (任意) 特定の VLAN グループにマッピングされている各 VLAN のユーザ数を表示します。
Command Modes	特権 EXEC (#)
Command History	リリース 変更内容
	Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

Usage Guidelines **show vlan group** コマンドは既存の VLAN グループを表示し、各 VLAN グループのメンバである VLAN および VLAN の範囲を示します。 **group-name** キーワードを入力すると、指定した VLAN グループのメンバのみが表示されます。

Examples

次の例では、特定の VLAN グループのメンバを表示する方法を示します。

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

次に、グループ内の各 VLAN のユーザ数を表示する例を示します。

```
Device# show vlan group group-name group2 user_count
```

```
VLAN      : Count
-----
40         : 5
41         : 8
42         : 12
43         : 2
44         : 9
45         : 0
```

ssci-based-on-sci

Secure Channel Identifier (SCI) 値に基づいて Short Secure Channel Identifier (SSCI) 値を計算するには、MKA ポリシー コンフィギュレーション モードで **ssci-based-on-sci** コマンドを使用します。SCI に基づく SSCI 計算を無効にするには、このコマンドの **no** 形式を使用します。

ssci-based-on-sci
no ssci-based-on-sci

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

SCI 値に基づく SSCI 値の計算は無効になっています。

Command Modes

MKA ポリシー コンフィギュレーション (config-mka-policy)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.3	このコマンドが導入されました。

Usage Guidelines

SCI 値が高いほど、SSCI 値は低くなります。

Examples

次に、SCI に基づく SSCI 計算を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# ssci-based-on-sci
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。

Command	Description
use-updated-eth-header	ICV 計算には更新されたイーサネットヘッダーを使用します。

switchport port-security aging

セキュアアドレスエントリのエージングタイムおよびタイプを設定する、または特定のポートのセキュアアドレスのエージング動作を変更するには、インターフェイス コンフィギュレーション モードで **switchport port-security aging** コマンドを使用します。ポート セキュリティ エージングをディセーブルにする、またはパラメータをデフォルトの状態に設定するには、このコマンドの **no** 形式を使用します。

```
switchport port-security aging {static|time time|type {absolute|inactivity}}
no switchport port-security aging {static|time|type}
```

Syntax Description

static	このポートに静的に設定されたセキュアアドレスのエージングをイネーブルにします。
time <i>time</i>	このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。 <i>time</i> が 0 の場合、このポートのエージングはディセーブルです。
type	エージング タイプを設定します。
absolute	absolute エージング タイプを設定します。このポートのすべてのセキュアアドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュアアドレス リストから削除されます。
inactivity	inactivity エージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータトラフィックがない場合だけ、このポートのセキュアアドレスが期限切れになります。

Command Default

ポート セキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。
デフォルトのエージング タイプは **absolute** です。
デフォルトのスタティック エージング動作はディセーブルです。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

特定のポートのセキュア アドレス エージングをイネーブルにするには、ポート エージング タイムを 0 以外の値に設定します。

特定のセキュアアドレスに時間を限定してアクセスできるようにするには、エージングタイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュア アドレスが削除されます。

継続的にアクセスできるセキュアアドレス数を制限するには、エージングタイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュアアドレスが削除され、他のアドレスがセキュアになることができます。

セキュアアドレスへのアクセス制限を解除するには、セキュアアドレスとして設定し、**noswitchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用して、静的に設定されたセキュアアドレスのエージングをディセーブルにします。

次の例では、ポートのすべてのセキュアアドレスに対して、エージングタイプを **absolute**、エージング タイムを 2 時間に設定します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
Device(config-if)# end
```

次の例では、ポートに設定されたセキュア アドレスに対して、エージング タイプを **inactivity**、エージング タイムを 2 分に設定します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
Device(config-if)# end
```

次の例では、設定されたセキュア アドレスのエージングをディセーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
Device(config-if)# end
```

switchport port-security mac-address

セキュア MAC アドレスまたはスティッキ MAC アドレスラーニングを設定するには、**switchport port-security mac-address** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport port-security mac-address {mac-address [vlan {vlan-id {access | voice}}]} | sticky
[mac-address | vlan {vlan-id {access | voice}}]}
no switchport port-security mac-address {mac-address [vlan {vlan-id {access | voice}}]} | sticky
[mac-address | vlan {vlan-id {access | voice}}]}
```

Syntax Description

mac-address 48 ビット MAC アドレスの入力によって指定するインターフェイスのセキュア MAC アドレス。設定された最大数まで、セキュア MAC アドレスを追加できます。

vlan vlan-id (任意) トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。

vlan access (任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。

vlan voice (任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。

Note **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

sticky スティックラーニングのインターフェイスをイネーブルにします。スティッキラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキセキュア MAC アドレスに変換します。

mac-address (任意) スティックセキュア MAC アドレスを指定する MAC アドレス。

Command Default

セキュア MAC アドレスは設定されていません。
スティッキ ラーニングはディセーブルです。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。

- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ（SPAN）の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは10ギガビットEtherChannelポートグループに含めることはできません。
- 音声VLANでは、スタティックセキュアまたはスティッキセキュアMACアドレスを設定できません。
- 音声VLANが設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を2に設定します。ポートをCisco IP Phoneに接続する場合は、IP PhoneにMACアドレスが1つ必要です。Cisco IP Phoneのアドレスは音声VLAN上で学習されますが、アクセスVLAN上では学習されません。1台のPCをCisco IP Phoneに接続する場合は、MACアドレスの追加は必要ありません。2台以上のPCをCisco IP Phoneに接続する場合は、各PCに1つ、さらにCisco IP Phoneに1つ割り当てるよう十分なセキュアアドレスを設定する必要があります。
- 音声VLANはアクセスポート上でだけサポートされます。トランクポート上ではサポートされません。

スティッキセキュアMACアドレスには、次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上でスティッキラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミックセキュアMACアドレス（スティッキラーニングがイネーブルになる前に動的に学習されたアドレスを含む）を、スティッキセキュアMACアドレスに変換し、すべてのスティッキセキュアMACアドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキセキュアMACアドレスは実行コンフィギュレーションの一部に残りますが、アドレステーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミックアドレスとしてアドレステーブルに追加されます。
- **switchport port-security mac-address sticky mac-address** インターフェイス コンフィギュレーション コマンドを使用して、スティッキセキュアMACアドレスを設定する場合、これらのアドレスはアドレステーブルおよび実行コンフィギュレーションに追加されます。ポートセキュリティがディセーブルの場合、スティッキセキュアMACアドレスは実行コンフィギュレーションに残ります。
- スティッキセキュアMACアドレスがコンフィギュレーションファイルに保存されていると、デバイスの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくて済みます。スティッキセキュアアドレスを保存しない場合、アドレスは失われます。スティッキラーニングがディセーブルの場合、スティッキ

セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

- ステイックラーニングをディセーブルにして、**switchport port-security mac-address sticky mac-address** インターフェイスコンフィギュレーションコマンドを入力した場合、エラーメッセージが表示され、ステイッキセキュア MAC アドレスは実行コンフィギュレーションに追加されません。

設定を確認するには、**show port-security** コマンドを使用します。

次の例では、ポートでセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
Device(config-if)# end
```

次の例では、ステイッキ ラーニングをイネーブルにして、ポート上で2つのステイッキセキュア MAC アドレスを入力する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
Device(config-if)# end
```

switchport port-security maximum

セキュア MAC アドレスの最大数を設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security maximum** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport port-security maximum value [vlan [vlan-list] [access | voice]]
no switchport port-security maximum value [vlan [vlan-list] [access | voice]]
```

Syntax Description

value インターフェイスのセキュア MAC アドレスの最大数を設定します。

デフォルトの設定は 1 秒です。

vlan (任意) トランク ポートの場合、VLAN ごとまたは一定範囲の VLAN のセキュア MAC アドレスの最大数を設定します。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。

vlan-list (任意) カンマで区切られた VLAN の範囲またはハイフンで区切られた一連の VLAN。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。

access (任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。

voice (任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。

Note **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

Command Default

ポートセキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 です。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デバイスに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。**sdm prefer** コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることができますが、ダイナミック アクセス ポートには設定できません。

- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ（SPAN）の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合は、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合は、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。

音声 VLAN はアクセスポート上でだけサポートされます。トランクポート上ではサポートされません。

- インターフェイスのセキュアアドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュアアドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

設定を確認するには、**show port-security** コマンドを使用します。

次の例では、ポートでポートセキュリティをイネーブルにし、セキュアアドレスの最大数を 5 に設定する方法を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

switchport port-security violation

セキュア MAC アドレスの違反モード、またはポートセキュリティに違反した場合に実行するアクションを設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security violation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security violation {protect|restrict|shutdown|shutdown vlan}
no switchport port-security violation {protect|restrict|shutdown|shutdown vlan}

Syntax Description

protect	セキュリティ違反保護モードを設定します。
restrict	セキュリティ違反制限モードを設定します。
shutdown	セキュリティ違反シャットダウン モードを設定します。
shutdown vlan	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。

Command Default

デフォルトの違反モードは **shutdown** です。

Command Modes

インターフェイス コンフィギュレーション (config-if)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

セキュリティ違反保護モードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスの packets はドロップされます。ドロップすることでセキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。



Note トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

セキュリティ違反制限モードでは、セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスの packets はドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。

セキュリティ違反シャットダウンモードでは、違反が発生し、ポートのLEDがオフになると、インターフェイスが **errdisable** になります。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュアポートが **errdisable** ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。

セキュリティ違反モードが VLAN ごとのシャットダウンに設定されると、違反が発生した VLAN のみが **errdisable** になります。

セキュアポートに関する制限事項は、次のとおりです。

- セキュアポートはアクセスポートまたはトランクポートにすることができますが、ダイナミックアクセスポートには設定できません。
- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。

セキュア MAC アドレスの最大値がアドレステーブルに存在し、アドレステーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュアポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起きます。

セキュアポートが **errdisable** ステートの場合は、**errdisable recovery cause psecure-violation** グローバルコンフィギュレーションコマンドを入力して、このステートから回復させることができます。**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、MACセキュリティ違反が発生した場合に VLAN のみをシャットダウンするようポートを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
Device(config)# exit
```

tacacs server

IPv6 または IPv4 用に TACACS+ サーバを設定し、TACACS+ サーバコンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **tacacs server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

```
tacacs server name
no tacacs server
```

Syntax Description

<i>name</i>	プライベート TACACS+ サーバホストの名前。
-------------	---------------------------

Command Default

TACACS+ サーバは構成されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

tacacs server コマンドは、*name* 引数を使用して TACACS サーバを設定し、TACACS+ サーバコンフィギュレーションモードを開始します。設定が完了し、TACACS+ サーバコンフィギュレーションモードを終了すると、設定が適用されます。

Examples

次の例は、名前 `server1` を使用して TACACS サーバを設定し、さらに設定を行うために TACACS+ サーバコンフィギュレーションモードを開始する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# end
```

Related Commands

Command	Description
address ipv6 (TACACS+)	TACACS+ サーバの IPv6 アドレスを設定します。
key (TACACS+)	TACACS+ サーバでサーバ単位の暗号キーを設定します。
port (TACACS+)	TACACS+ 接続に使用する TCP ポートを指定します。
send-nat-address (TACACS+)	クライアントの NAT 後のアドレスを TACACS+ サーバに送信します。
single-connection (TACACS+)	単一の TCP 接続を使用してすべての TACACS パケットを同じサーバに送信できるようにします。

Command	Description
timeout(TACACS+)	指定された TACACS サーバからの応答を待機する時間を設定します。

token (パラメータマップ)

デバイス登録で承認に使用するアプリケーションプログラミング インターフェイス (API) キーを設定するには、パラメータマップタイプ検査コンフィギュレーション モードで **token** コマンドを使用します。固有識別子を削除するには、このコマンドの **no** 形式を使用します。

token *value*
no token

Syntax Description	<i>value</i>	API トークン。これは Cisco Umbrella 登録サーバから取得できます。
Command Default	パラメータマップのトークンは作成されていません。	
Command Modes	パラメータマップタイプ検査コンフィギュレーション (config-profile)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。
Usage Guidelines	<p>token コマンドは、umbrella in および umbrella out コマンドに対する必須の設定です。</p> <p>既存のトークンを新しいトークンに変更するには、umbrella in コマンドを削除し、適用する新しいトークンのポリシーに対応するようにインターフェイスで再設定します。</p>	
Examples	<p>次に、Cisco Umbrella のトークンを設定する例を示します。</p> <pre>Device> enable Device# configure terminal Device(config)# parameter-map type umbrella global Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEFF</pre>	
Related Commands	コマンド	説明
	parameter-map type umbrella global	Umbrella モードでパラメータマップタイプを設定します。
	umbrella	インターフェイスで Cisco Umbrella Connector を設定します。

tracking (IPv6 スヌーピング)

ポートでデフォルトのトラッキングポリシーを上書きするには、IPv6 スヌーピングポリシーコンフィギュレーションモードで **tracking** コマンドを使用します。

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

Syntax Description	
enable	トラッキングをイネーブルにします。
reachable-lifetime	<p>(任意) 到達可能という証明がない状態で、到達可能なエントリが直接的または間接的に到達可能であると判断される最大時間を指定します。</p> <ul style="list-style-type: none"> • reachable-lifetime キーワードを使用できるのは、enable キーワードが指定されている場合のみです。 • reachable-lifetime キーワードを使用すると、ipv6 neighbor binding reachable-lifetime コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。
<i>value</i>	秒単位のライフタイム値。指定できる範囲は 1 ~ 86400 で、デフォルトは 300 です。
infinite	エントリを無限に到達可能状態またはステイル状態に維持します。
disable	トラッキングをディセーブルにします。
stale-lifetime	<p>(任意) 時間エントリをステイル状態に維持します。これによりグローバルの stale-lifetime 設定が上書きされます。</p> <ul style="list-style-type: none"> • ステイル ライフタイムは 86,400 秒です。 • stale-lifetime キーワードを使用できるのは、disable キーワードが指定されている場合のみです。 • stale-lifetime キーワードを使用すると、ipv6 neighbor binding stale-lifetime コマンドで設定されたグローバルなステイルライフタイムが上書きされます。
Command Default	時間のエントリは到達可能な状態に維持されます。
Command Modes	IPv6 スヌーピング コンフィギュレーション (config-ipv6-snooping)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **tracking** コマンドは、このポリシーが適用されるポート上で **ipv6 neighbor tracking** コマンドによって設定されたデフォルトのトラッキングポリシーに優先します。この機能は、たとえば、エントリーを追跡しないが、バインディングテーブルにエントリーを残して盗難を防止する場合などに、信頼できるポート上で有用です。

reachable-lifetime キーワードは、到達可能という証明がない状態で、あるエントリーがトラッキングにより直接的に、または IPv6 スヌーピングにより間接的に到達可能であると判断される最大時間を示します。**reachable-lifetime** 値に到達すると、エントリーはステイル状態に移行します。**tracking** コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。

stale-lifetime キーワードは、エントリーが削除されるか、直接または間接的に到達可能であると証明される前にテーブルに保持される最大時間です。**tracking** コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイルライフタイムが上書きされます。

次に、IPv6 スヌーピングポリシー名を **policy1** と定義し、エントリーを信頼できるポート上で無限にバインディングテーブルに保存するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
Device(config-ipv6-snooping)# end
```

trusted-port

あるポートを信頼できるポートとして設定するには、IPv6 スヌーピング ポリシー モードまたは ND インスペクション ポリシー コンフィギュレーション モードで **trusted-port** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

trusted-port
no trusted-port

Syntax Description

このコマンドには、引数またはキーワードはありません。

Command Default

どのポートも信頼されていません。

Command Modes

ND インスペクション ポリシー コンフィギュレーション (config-nd-inspection)
IPv6 スヌーピング コンフィギュレーション (config-ipv6-snooping)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

trusted-port コマンドをイネーブルにすると、メッセージがこのポリシーを持つポートで受信された場合、限定的に実行されるか、まったく実行されません。ただし、アドレススプーフィングから保護するために、メッセージは伝送するバインディング情報の使用によってバインディングテーブルを維持できるように分析されます。これらのポートで検出されたバインディングは、信頼できるものとして設定されていないポートから受信したバインディングよりも信頼性が高いものと見なされます。

次に、NDP ポリシー名を `policy1` と定義し、ポートを信頼するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
Device(config-nd-inspection)# end
```

次に、IPv6 スヌーピングポリシー名を `policy1` と定義し、ポートを信頼するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
Device(config-ipv6-snooping)# end
```

umbrella

インターフェイスで Cisco Umbrella Connector を設定するには、インターフェイス コンフィギュレーションモードで **umbrella** コマンドを使用します。この設定を削除するには、このコマンドの **no** 形式を使用します。

umbrella {**in** *tag-name* | **out**}

no umbrella {**in** | **out**}

Syntax Description	in	クライアントに接続されているインターフェイスで Cisco Umbrella Connector を設定します。
	<i>tag-name</i>	インターフェイスタグ名。 長さは 49 文字までです。
	out	Umbrella サーバに到達するために使用されるインターフェイスで Cisco Umbrella Connector を設定します。
Command Default	デフォルトの動作や値はありません。	
Command Modes	インターフェイス コンフィギュレーション (config-if)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

Usage Guidelines **umbrella in** コマンドを設定する前に、**umbrella out** コマンドを設定する必要があります。登録は、ポート 443 がオープン状態にあり、既存のファイアウォールへのトラフィックのパススルーが許可される場合にのみ成功します。

umbrella in コマンドと **umbrella out** コマンドを同じインターフェイスで設定することはできません。

Examples

次に、インターフェイスで Cisco Umbrella Connector を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# umbrella out
Device(config-if)# exit
Device(config)# interface GigabitEthernet 1/0/2
Device(config-if)# umbrella in mydevice_tag
```

Related Commands

コマンド	説明
show umbrella config	デバイスの Cisco Umbrella 統合設定を表示します。

use-updated-eth-header

整合性チェック値（ICV）の計算のために MACsec Key Agreement Protocol Data Unit（MKPDU）の更新されたイーサネットヘッダーを含むデバイスとデバイス上の任意のポートの間の相互運用性を有効にするには、MKA ポリシーコンフィギュレーションモードで **ssci-based-on-sci** コマンドを使用します。ICV 計算のために MKPDU の更新されたイーサネットヘッダーを無効にするには、このコマンドの **no** 形式を使用します。

use-updated-eth-header
no use-updated-eth-header

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default ICV 計算のためのイーサネットヘッダーは無効になっています。

Command Modes MKA ポリシー コンフィギュレーション（config-mka-policy）

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

Usage Guidelines 更新されたイーサネットヘッダーは非標準です。このオプションを有効にすると、デバイス間の MACsec Key Agreement（MKA）セッションを設定できます。

Examples

次に、ICV 計算のために MKPDU の更新されたイーサネットヘッダーを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# use-updated-eth-header
```

Related Commands

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。

Command	Description
send-secure-announcements	MKPDUの送信でセキュアなアナウンスを送信するようにMKAを設定します。
ssci-based-on-sci	SCIに基づいてSSCIを計算します。

username

ユーザ名ベースの認証システムを確立するには、グローバル コンフィギュレーション モードで **username** コマンドを使用します。確立されたユーザ名ベースの認証を削除するには、このコマンドの **no** 形式を使用します。

```
username name [aaa attribute list aaa-list-name]
username name[access-class access-list-number]
username name[algorithm-type {md5 | scrypt | sha256}]
username name[autocommand command]
username name[callback-dialstring telephone-number]
username name[callback-line [tty ]line-number [ending-line-number]]
username name[callback-rotary rotary-group-number]
username name[common-criteria-policy policy-name]
username name[dnis]
username name[mac]
username name[nocallback-verify]
username name[noescape]
username name[nohangup]
username name[nopassword | password password | password encryption-type encrypted-password]
username name[one-time {password {0 | 6 | 7 |password} | secret {0 | 5 | 8 | 9 |password}}]
username name[password secret]
username name[privilege level]
username name[secret {0 | 5 |password}]
username name[serial-number]
username name[user-maxlinks number]
username name[view view-name]
no username name
```

Syntax Description

<i>name</i>	ホスト名、サーバ名、ユーザ ID、またはコマンド名。 <i>name</i> 引数には1つの単語だけ使用できます。空白や引用符は使用できません。
aaa attribute list <i>aaa-list-name</i>	(任意) 指定した認証、許可、およびアカウントिंग (AAA) 方式リストを使用します。
access-class <i>access-list-number</i>	(任意) ライン コンフィギュレーション モードで使用可能な access-class コマンドで指定されたアクセスリストをオーバーライドする発信アクセスリストを指定します。これはユーザのセッションで使用されます。
algorithm-type	(任意) ユーザのプレーンテキストのシークレットをハッシュするために使用するアルゴリズムを指定します。 <ul style="list-style-type: none"> • md5: MD5 アルゴリズムを使用してパスワードをエンコードします。 • scrypt: SCRYPT ハッシュアルゴリズムを使用してパスワードをエンコードします。 • sha256: PBKDF2 ハッシュアルゴリズムを使用してパスワードをエンコードします。

autocommand <i>command</i>	(任意) 指定した autocommand コマンドがユーザのログイン後に自動的に発行されるようにします。指定した autocommand コマンドが完了するとセッションが終了します。このコマンドは任意の長さに行うことができ、途中にスペースを含めることもできるため、 autocommand キーワードを使用するコマンドは行の最後のオプションにする必要があります。
callback-dialstring <i>telephone-number</i>	(任意) データ回線終端装置 (DCE) デバイスに渡す電話番号を指定できます (非同期コールバックの場合のみ)。
callback-line <i>line-number</i>	(任意) 特定のユーザ名をコールバックに対して有効にする端末回線 (または連続したグループの最初の回線) の相対番号を指定します (非同期コールバックの場合のみ)。番号はゼロから始まります。
<i>ending-line-number</i>	(任意) 特定のユーザ名をコールバックに対して有効にする連続したグループの最後の回線の相対番号。キーワード (tty など) を省略した場合、 line-number および ending-line-number は相対回線番号ではなく絶対回線番号となります。
tty	(任意) 標準の非同期回線を指定します (非同期コールバックの場合のみ)。
callback-rotary <i>rotary-group-number</i>	(任意) 特定のユーザ名をコールバックに対して有効にするロータリーグループ番号を指定できます (非同期コールバックの場合のみ)。ロータリーグループで次に使用可能な回線が選択されます。範囲は 1 ~ 100 です。
common-criteria-policy	(任意) コモンクライテリアポリシーの名前を指定します。
dnis	(任意) 着信番号識別サービス (DNIS) から取得された場合にパスワードを不要にします。
mac	(任意) MAC アドレスをローカルで実行される MAC フィルタリングのユーザ名として使用できるようにします。
nocallback-verify	(任意) 指定した回線の EXEC コールバックに認証が不要であることを指定します。
noescape	(任意) ユーザが接続されているホストでエスケープ文字を使用できないようにします。
nohangup	(任意) 自動コマンド (autocommand キーワードを使用して設定) の実行後に Cisco IOS ソフトウェアでユーザを切断しないようにします。ユーザには、代わりに別のユーザ EXEC プロンプトが表示されます。
nopassword	(任意) ユーザがログインする際のパスワードを不要にします。通常、このキーワードは autocommand キーワードを使用する場合に組み合わせて使用すると役立ちます。

password	(任意) <i>name</i> 引数にアクセスするためのパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、 username コマンドの最後のオプションとして指定します。
<i>password</i>	ユーザが入力するパスワード。
<i>encryption-type</i>	password の直後のテキストが暗号化されるかどうか、および暗号化される場合は使用される暗号化タイプを定義する 1 桁の数字。定義されている暗号化タイプは、0 (password の直後のテキストは暗号化されない) および 6 と 7 (テキストはシスコが定義した暗号化アルゴリズムを使用して暗号化される) です。
<i>encrypted-password</i>	ユーザが入力する暗号化パスワード。
one-time	(任意) ユーザ名とパスワードが 1 回だけ有効であることを指定します。この設定は、デフォルトのクレデンシャルがユーザ設定に残らないようにするために使用されます。 <ul style="list-style-type: none"> • 0: 暗号化されていないパスワードまたはシークレット (設定に依存) が続くことを指定します。 • 6: 暗号化パスワードが続くことを指定します。 • 7: 非表示のパスワードが続くことを指定します。 • 5: MD5 でハッシュされたシークレットが続くことを指定します。 • 8: PBKDF2 でハッシュされたシークレットが続くことを指定します。 • 9: SCRYPT でハッシュされたシークレットが続くことを指定します。
secret	(任意) ユーザのシークレットを指定します。
<i>secret</i>	チャレンジハンドシェイク認証プロトコル (CHAP) 認証に使用します。ローカルデバイスまたはリモートデバイスのシークレットを指定します。シークレットはローカルデバイスに暗号化されて格納されます。最大 11 文字の ASCII 文字からなる任意の文字列で構成できます。指定できるユーザ名とパスワードの組み合わせの数に制限はないため、任意の数のリモートデバイスを認証できます。
privilege <i>privilege-level</i>	(任意) ユーザの特権レベルを設定します。範囲: 1 ～ 15。
serial-number	(任意) シリアル番号を指定します。
user-maxlinks <i>number</i>	(任意) ユーザに許可されるインバウンドリンクの最大数を指定します。
view <i>view-name</i>	(任意) parser view コマンドで指定された CLI ビュー名をローカル AAA データベースに関連付けます (CLI ビューの場合のみ)。

Command Default	ユーザ名に基づく認証システムは確立されません。	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更
	Cisco IOS XE Fuji 16.9.2	この した。

Usage Guidelines **username** コマンドは、ログインだけを目的としてユーザ名、パスワード、またはその両方の認証を行います。

複数の **username** コマンドを使用して、単一ユーザのオプションを指定できます。

ローカルデバイスと通信を行う、認証が必要になるリモートシステムごとに、ユーザ名のエントリを追加します。リモートデバイスには、ローカルデバイスのユーザ名のエントリが必要です。このエントリは、そのリモートデバイスに対応するローカルデバイスのエントリと同じパスワードにする必要があります。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する *info* ユーザ名を定義できます。

username コマンドは、CHAP の設定の一部として必要です。ローカルデバイスが認証を必要とするリモートシステムごとにユーザ名のエントリを追加します。

ローカルデバイスをリモートの CHAP チャレンジに応答できるようにするには、一方の **username name** エントリを他方のデバイスにすでに割り当てられている **hostname** エントリと同じにする必要があります。権限レベル 1 のユーザが上位の権限レベルを開始する状況を回避するには、ユーザ単位の権限レベルを 1 以外に設定します（たとえば 0 または 2 ~ 15）。ユーザ単位の権限レベルは仮想端末の権限レベルよりも優先されます。

CLI ビューと合法的傍受ビュー

CLI ビューと合法的傍受ビューは、どちらも特定のコマンドと設定情報へのアクセスを制限します。合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する SNMP コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

lawful-intercept キーワードを使用して指定されたユーザは、他の権限レベルまたはビュー名が明示的に指定されていない場合、デフォルトで合法的傍受ビューになります。

secret 引数に値が指定されていない場合、**debug serial-interface** コマンドが有効になっていると、リンクの確立時にエラーが表示され、CHAP チャレンジは実装されません。CHAP デバッグ情報は、**debug ppp negotiation**、**debug serial-interface**、および **debug serial-packet** コマンドを使用して確認できます。

Examples

次に、ログインプロンプトで入力できる UNIX の **who** コマンドに似た、デバイスの現在のユーザを一覧表示するサービスを実装する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username who nopassword nohangup autocommand show users
```

次に、パスワードを使用する必要がない情報サービスを実装する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username info nopassword noescape autocommand telnet nic.ddn.mil
```

次に、すべての TACACS+ サーバが切断された場合でも機能する ID を実装する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username superuser password superpassword
```

次に、server_1 のシリアルインターフェイス 0 で CHAP を有効にする例を示します。server_r という名前のリモートサーバのパスワードも定義しています。

```
hostname server_1
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次に、暗号化されたパスワードを表示する **show running-config** コマンドの出力例を示します。

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次に、権限レベル 1 のユーザによる 1 よりも高い権限レベルへのアクセスを拒否する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username user privilege 0 password 0 cisco
Device(config)# username user2 privilege 2 password 0 cisco
```

次に、user2 のユーザ名ベースの認証を削除する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no username user2
```

Related Commands

Command	Description
debug ppp negotiation	PPP の始動時に、PPP オプションをネゴシエートするためパケットを表示します。

Command	Description
debug serial-interface	シリアル接続の障害に関する情報を表示します。
debug serial-packet	debug serial interface コマンドを使用して取得できる情報。ルインターフェイスのデバッグ情報を表示します。

vlan access-map

VLAN パケットフィルタリング用の VLAN マップエントリを作成または修正し、VLAN アクセス マップ コンフィギュレーション モードに変更するには、デバイス上でグローバル コンフィギュレーション モードで **vlan access-map** コマンドを使用します。VLAN マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

```
vlan access-map name [number]
no vlan access-map name [number]
```

Syntax Description

<i>name</i>	VLAN マップ名
<i>number</i>	(任意) 作成または変更するマップ エントリのシーケンス番号 (0 ~ 65535)。VLAN マップを作成する際にシーケンス番号を指定しない場合、番号は自動的に割り当てられ、10 から開始して 10 ずつ増加します。この番号は、VLAN アクセス マップ エントリに挿入するか、または VLAN アクセス マップ エントリから削除する順番です。

Command Default

VLAN に適用する VLAN マップ エントリまたは VLAN マップはありません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

グローバル コンフィギュレーション モードでは、このコマンドは VLAN マップを作成または修正します。このエントリは、モードを VLAN アクセス マップ コンフィギュレーションに変更します。**match** アクセス マップ コンフィギュレーション コマンドを使用して、照合する IP または非 IP トラフィックのアクセスリストを指定できます。また、**action** コマンドを使用して、この照合によりパケットを転送またはドロップするかどうかを設定します。

VLAN アクセス マップ コンフィギュレーション モードでは、次のコマンドが利用できます。

- **action:** 実行するアクションを設定します (転送またはドロップ)。
- **default:** コマンドをデフォルト値に設定します。
- **exit:** VLAN アクセス マップ コンフィギュレーション モードを終了します。
- **match:** 照合する値を設定します (IP アドレスまたは MAC アドレス)。
- **no:** コマンドを無効にするか、デフォルト値を設定します。

エントリ番号 (シーケンス番号) を指定しない場合、マップの最後に追加されます。

VLAN ごとに VLAN マップは 1 つだけ設定できます。VLAN マップは、VLAN でパケットを受信すると適用されます。

シーケンス番号を指定して **no vlan access-map name [number]** コマンドを使用すると、エントリを個別に削除できます。

VLAN マップを1つまたは複数の VLAN に適用するには、**vlan filter** インターフェイス コンフィギュレーション コマンドを使用します。

Examples

次の例では、**vac1** という名の VLAN マップを作成し、一致条件とアクションをその VLAN マップに適用する方法を示します。他のエントリがマップに存在しない場合、これはエントリ 10 になります。

```
Device> enable
Device# configure terminal
Device(config)# vlan access-map vac1
Device(config-access-map)# match ip address acl1
Device(config-access-map)# action forward
Device(config-access-map)# end
```

次の例では、VLAN マップ **vac1** を削除する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# no vlan access-map vac1
Device(config)# exit
```

vlan dot1Q tag native

トランクポートのネイティブ VLAN で dot1q (IEEE 802.1Q) のタグリングを有効にするには、グローバル コンフィギュレーション モードで **vlan dot1Q tag native** コマンドを使用します。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

vlan dot1Q tag native
no vlan dot1Q tag native

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デイセーブル

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

Usage Guidelines 通常は、ネイティブ VLAN ID で 802.1Q トランクを設定します。これによって、その VLAN 上のすべてのパケットからタグリングが取り除かれます。

ネイティブ VLAN でのタグリングを維持し、タグなしトラフィックをドロップするには、**vlan dot1q tag native** コマンドを使用します。デバイスによって、ネイティブ VLAN で受信したトラフィックがタグ付けされ、802.1Q タグが付けられたフレームのみが許可され、ネイティブ VLAN のタグなしトラフィックを含むすべてのタグなしトラフィックはドロップされます。

vlan dot1q tag native コマンドがイネーブルになっていても、トランクポートのネイティブ VLAN では、制御トラフィックはタグなしとして引き続き許可されます。



Note **dot1q tag vlan native** コマンドがグローバルレベルで設定されている場合、トランクポートでの dot1x 再認証は失敗します。

次に、デバイスのすべてのトランクポートでネイティブ VLAN の dot1q (IEEE 802.1Q) タグリングを有効にする例を示します。

```
Device(config)# vlan dot1q tag native
Device(config)#
```

Related Commands

Command	Description
show vlan dot1q tag native	ネイティブ VLAN のタグリングのステータスを表示します。

vlan filter

VLAN マップを 1 つまたは複数の VLAN に適用するには、グローバル コンフィギュレーション モードで **vlan filter** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

```

vlan filter mapname vlan-list {list | all}
no vlan filter mapname vlan-list {list | all}

```

Syntax Description	
mapname	VLAN マップ エントリ名
vlan-list	マップを適用する VLAN を指定します。
リスト	tt、uu-vv、xx、および yy-zz 形式での 1 つまたは複数の VLAN リスト。カンマとダッシュの前後のスペースは任意です。指定できる範囲は 1 ~ 4094 です。
all	マップをすべての VLAN に追加します。

Command Default VLAN フィルタはありません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines パケットを誤って過剰にドロップし、設定プロセスの途中で接続が無効にならないように、VLAN アクセス マップを完全に定義してから VLAN に適用することを推奨します。

Examples

次の例では、VLAN マップ エントリ map1 を VLAN 20 および 30 に適用します。

```

Device> enable
Device# configure terminal
Device(config)# vlan filter map1 vlan-list 20, 30
Device(config)# exit

```

次の例では、VLAN マップ エントリ map1 を VLAN 20 から削除する方法を示します。

```

Device> enable
Device# configure terminal
Device(config)# no vlan filter map1 vlan-list 20
Device(config)# exit

```

設定を確認するには、**show vlan filter** コマンドを入力します。

vlan group

VLAN グループを作成または変更するには、グローバル コンフィギュレーション モードで **vlan group** コマンドを使用します。VLAN グループから VLAN リストを削除するには、このコマンドの **no** 形式を使用します。

```
vlan group group-name vlan-list vlan-list
no vlan group group-name vlan-list vlan-list
```

Syntax Description	group-name	VLAN グループの名前。名前は最大 32 文字で、文字から始める必要があります。
	vlan-list vlan-list	VLAN グループに追加される 1 つ以上の VLAN を指定します。vlan-list 引数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲を指定できます。複数のエントリはハイフン (-) またはカンマ (,) で区切ります。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 指定された VLAN グループが存在しない場合、**vlan group** コマンドはグループを作成し、指定された VLAN リストをそのグループにマッピングします。指定された VLAN グループが存在する場合は、指定された VLAN リストがそのグループにマッピングされます。

vlan group コマンドの **no** 形式を使用すると、指定された VLAN リストが VLAN グループから削除されます。VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されません。

最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。

Examples

次に、VLAN 7～9 と 11 を VLAN グループにマッピングする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# vlan group group1 vlan-list 7-9,11
Device(config)# exit
```

次の例では、VLAN グループから VLAN 7 を削除する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# no vlan group group1 vlan-list 7
Device(config)# exit
```



PART **XI**

スタックマネージャおよびハイアベイラビリティ

- [スタックマネージャおよびハイアベイラビリティ コマンド](#), on page 1655



スタックマネージャおよびハイアベイラビリティコマンド

- [main-cpu](#), on page 1656
- [mode sso](#), on page 1657
- [policy config-sync prc reload](#), on page 1658
- [redundancy](#), on page 1659
- [redundancy config-sync mismatched-commands](#), on page 1660
- [redundancy force-switchover](#), on page 1662
- [redundancy reload](#), on page 1663
- [reload](#), on page 1664
- [show redundancy](#), on page 1665
- [show redundancy config-sync](#), on page 1669
- [show switch](#), on page 1671
- [show switch stack-mode](#), on page 1677
- [stack-mac persistent timer](#), on page 1678
- [stack-mac update force](#), on page 1680
- [standby console enable](#), on page 1681
- [switch clear stack-mode](#), on page 1682
- [switch switch-number role](#), on page 1683
- [switch stack port](#), on page 1684
- [switch priority](#), on page 1686
- [switch provision](#), on page 1687
- [switch renumber](#), on page 1689
- [switch renumber](#), on page 1690

main-cpu

冗長メインコンフィギュレーションサブモードを開始し、スタンバイをイネーブルにするには、冗長コンフィギュレーションモードで **main-cpu** コマンドを使用します。

main-cpu

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes 冗長コンフィギュレーション (config-red)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 冗長メイン コンフィギュレーションサブモードから、**standby console enable** コマンドを使用してスタンバイをイネーブルにします。

次に、冗長メイン コンフィギュレーションサブモードを開始し、スタンバイをイネーブルにする例を示します。

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device#
```

mode sso

冗長モードをステートフルスイッチオーバー（SSO）に設定するには、冗長コンフィギュレーションモードで **mode sso** コマンドを使用します。

mode sso

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes 冗長コンフィギュレーション

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **mode sso** コマンドは、冗長コンフィギュレーションモードでのみ入力できます。

システムを SSO モードに設定する場合は、次の注意事項に従ってください。

- SSO モードをサポートするために、では同一の Cisco IOS イメージを使用する必要があります。Cisco IOS リリース間の相違のために、冗長機能が動作しない場合があります。
- モジュールの活性挿抜（OIR）を実行する場合、モジュールの状態が移行状態（Ready 以外の状態）である場合にだけ、ステートフルスイッチオーバーの間にスイッチはリセットし、ポートステートは再起動します。
- 転送情報ベース（FIB）テーブルはスイッチオーバー時に消去されます。ルーテッドトラフィックは、ルートテーブルが再コンバージェンスするまで中断されます。

次の例では、冗長モードを SSO に設定する方法を示します。

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)#
```

policy config-sync prc reload

Parser Return Code (PRC) の障害がコンフィギュレーションの同期中に発生した場合にスタンバイをリロードするには、冗長コンフィギュレーションモードで **policy config-sync reload** コマンドを使用します。Parser Return Code (PRC) の障害が発生した場合にスタンバイがリロードしないように指定するには、このコマンドの **no** 形式を使用します。

```
policy config-sync {bulk | lbl} prc reload
no policy config-sync {bulk | lbl} prc reload
```

Syntax Description	bulk バルク コンフィギュレーション モードを指定します。
	lbl 1 行ごと (lbl) のコンフィギュレーションモードを指定します。
Command Default	このコマンドは、デフォルトではイネーブルです。
Command Modes	冗長コンフィギュレーション (config-red)
Command History	リリース 変更内容
	Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

次に、Parser Return Code (PRC) の障害がコンフィギュレーションの同期化中に発生した場合に、スタンバイがリロードされないように指定する例を示します。

```
Device(config-red)# no policy config-sync bulk prc reload
```

redundancy

冗長コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **redundancy** コマンドを使用します。

redundancy

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes グローバルコンフィギュレーション (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 冗長コンフィギュレーションモードは、スタンバイをイネーブルにするために使用されるメインCPUサブモードを開始するために使用されます。

メインCPUサブモードを開始するには、冗長コンフィギュレーションモードで **main-cpu** コマンドを使用します。

スタンバイを有効にするには、メインCPUサブモードから **standby console enable** コマンドを使用します。

冗長コンフィギュレーションモードを終了するには、**exit** コマンドを使用します。

次に、冗長コンフィギュレーションモードを開始する例を示します。

```
デバイス(config)# redundancy
デバイス(config-red)#
```

次の例では、メインCPUサブモードを開始する方法を示します。

```
デバイス(config)# redundancy
デバイス(config-red)# main-cpu
デバイス(config-r-mc)#
```

Related Commands	コマンド	説明
	show redundancy	冗長ファシリティ情報を表示します。

redundancy config-sync mismatched-commands

アクティブスイッチとスタンバイスイッチの間に設定の不一致があるときにスタンバイスイッチのスタックへの参加を許可するには、特権 EXEC モードで **redundancy config-sync mismatched-commands** コマンドを使用します。

redundancy config-sync {ignore|validate} mismatched-commands

Syntax Description	ignore Mismatched Command List を無視します。
	validate 修正した実行コンフィギュレーションに基づいて Mismatched Command List を再確認します。
Command Default	なし
Command Modes	特権 EXEC
Command History	リリース 変更内容
	Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

Usage Guidelines スタンバイスイッチの起動中にアクティブスイッチの実行コンフィギュレーションのコマンド構文チェックが失敗した場合、**redundancy config-sync mismatched-commands** コマンドを使用して、アクティブスイッチの Mismatched Command List (MCL) を表示し、スタンバイスイッチをリブートします。

次に、不一致コマンドのログ エントリの例を示します。

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
! <submode> "interface"
- ip address 192.0.2.0 255.255.255.0
! </submode> "interface"
```

すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブスイッチの実行コンフィギュレーションからすべての不一致コマンドを除外します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイスイッチをリロードします。

次の手順に従って、MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイスイッチをリロードします。システムは SSO モードに移行します。



Note 不一致コマンドを無視する場合、アクティブスイッチとスタンバイスイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視された MCL は、**show redundancy config-sync ignored mcl** コマンドを使用して確認できません。

コンフィギュレーションファイルの互換性の問題が原因で、アクティブスイッチとスタンバイスイッチ間で SSO モードを確立できない場合、Mismatched Command List (MCL) がアクティブスイッチで生成され、スタンバイスイッチに対して Route Processor Redundancy (RPR) モードへのリロードが強制されます。

次の例に、変更したコンフィギュレーションとの Mismatched Command List を再検証する方法を示します。

```
デバイス# redundancy config-sync validate mismatched-commands
デバイス#
```

redundancy force-switchover

アクティブスイッチからスタンバイスイッチへのスイッチオーバーを強制的に実行するには、特権 EXEC モードで **redundancy force-switchover** コマンドを使用します。

redundancy force-switchover

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes 特権 EXEC (#)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 手動で冗長スイッチに切り替えるには、**redundancy force-switchover** コマンドを使用します。冗長スイッチは Cisco IOS XE イメージを実行する新しいアクティブスイッチになり、モジュールはデフォルト設定にリセットされます。古いアクティブスイッチは新しいイメージで再起動します。

アクティブスイッチで **redundancy force-switchover** コマンドを使用すると、アクティブスイッチのスイッチポートがダウン状態になります。

部分リング スタック内のスイッチにこのコマンドを使用すると、次の警告メッセージが表示されます。

```
Device# redundancy force-switchover

Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

次の例では、アクティブスーパーバイザエンジンからスタンバイスーパーバイザエンジンに手動で切り替える方法を示します。

```
Device# redundancy force-switchover
Device#
```

redundancy reload

スタック内のいずれか、またはすべてのスイッチを強制リロードするには、特権 EXEC モードで **redundancy reload** コマンドを使用します。

redundancy reload {peer | shelf}

Syntax Description

peer ピア ユニットをリロードします。

shelf スタック内のすべてのスイッチが再起動します。

Command Default

なし

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドを使用する前に、詳細情報についての「Performing a Software Upgrade」の項を参照してください。

スタック内のすべてのスイッチをリブートするには、**redundancy reload shelf** コマンドを使用します。

次に、手動でスタック内のすべてのスイッチをリロードする例を示します。

```
デバイス# redundancy reload shelf
デバイス#
```

reload

をリロードし、設定変更を適用するには、特権 EXEC モードで **reload** コマンドを使用します。

reload [/noverify | /verify] [*LINE* | **at** | **cancel** | **in**]

Syntax Description	
/noverify	(任意) リロードの前にファイル シグニチャを確認しないように指定します。
/verify	(任意) リロードの前にファイル シグニチャを確認します。
<i>LINE</i>	(任意) リセットの理由。
at	(任意) リロードを実行する時間を hh:mm 形式で指定します。
cancel	(任意) 保留中のリロードをキャンセルします。
in	(任意) リロードを実行する間隔を指定します。

Command Default をただちにリロードし、設定の変更を有効にします。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

show redundancy

冗長ファシリティ情報を表示するには、特権 EXEC モードで **show redundancy** コマンドを使用します。

show redundancy [**clients** | **config-sync** | **counters** | **history** [**reload** | **reverse**]] | {**clients** | **counters**} | **states** | **switchover history** [**domain default**]]

Syntax Description					
clients	(任意) 冗長ファシリティ クライアントに関する情報を表示します。				
config-sync	(任意) コンフィギュレーション同期の失敗または無視された Mismatched Command List (MCL) を表示します。				
counters	(任意) 冗長ファシリティ カウンタに関する情報を表示します。				
history	(任意) 冗長ファシリティの過去のステータスのログおよび関連情報を表示します。				
history reload	(任意) 冗長ファシリティの過去のリロード情報を表示します。				
history reverse	(任意) 冗長ファシリティの過去のステータスおよび関連情報のログを逆順で表示します。				
clients	指定セカンダリスイッチのすべての冗長ファシリティクライアントを表示します。				
counters	指定スタンバイスイッチのすべてのカウンタが表示されます。				
states	(任意) 冗長ファシリティの状態 (ディセーブル、初期化、スタンバイ、アクティブなど) に関する情報を表示します。				
switchover history	(任意) 冗長ファシリティのスイッチオーバー履歴に関する情報を表示します。				
domain default	(任意) スイッチオーバー履歴を表示するドメインとしてデフォルトドメインを表示します。				
Command Default	なし				
Command Modes	特権 EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

次の例では、冗長ファシリティに関する情報を表示する方法を示します。

```

Device# show redundancy

Redundant System Information :
-----
    Available system uptime = 1 hour, 25 minutes
Switchovers system experienced = 0
    Standby failures = 0
    Last switchover reason = not known

    Hardware Mode = Duplex
Configured Redundancy Mode = SSO
    Operating Redundancy Mode = SSO
    Maintenance Mode = Disabled
    Communications = Up

Current Processor Information :
-----
    Active Location = slot 1
    Current Software state = ACTIVE
    Uptime in current state = 1 hour, 25 minutes
    Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_LITE_IOSXE), Version 16.9.x
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sat 29-S
    Configuration register = 0x102

Peer Processor Information :
-----
    Standby Location = slot 3
    Current Software state = STANDBY HOT
    Uptime in current state = 1 hour, 22 minutes
    Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_LITE_IOSXE), Version 16.9.x
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sat 29-S
    Configuration register = 0x102

```

```
Device#
```

次の例では、冗長ファシリティクライアント情報を表示する方法を示します。

```

Device# show redundancy clients

Group ID =      1
  clientID = 29      clientSeq = 60      Redundancy Mode RF
  clientID = 139     clientSeq = 62      IfIndex
  clientID = 25      clientSeq = 71      CHKPT RF
  clientID = 10001   clientSeq = 85      QEMU Platform RF
  clientID = 77      clientSeq = 87      Event Manager
  clientID = 1340    clientSeq = 104     RP Platform RF
  clientID = 1501    clientSeq = 105     CWAN HA
  clientID = 78      clientSeq = 109     TSPTUN HA
  clientID = 305     clientSeq = 110     Multicast ISSU Consolidation RF
  clientID = 304     clientSeq = 111     IP multicast RF Client
  clientID = 22      clientSeq = 112     Network RF Client
  clientID = 88      clientSeq = 113     HSRP
  clientID = 114     clientSeq = 114     GLBP
  clientID = 225     clientSeq = 115     VRRP
  clientID = 4700    clientSeq = 118     COND_DEBUG RF
  clientID = 1341    clientSeq = 119     IOSXE DPIDX
  clientID = 1505    clientSeq = 120     IOSXE SPA TSM
  clientID = 75      clientSeq = 130     Tableid HA
  clientID = 501     clientSeq = 137     LAN-Switch VTP VLAN

```

<output truncated>

出力には、次の情報が表示されます。

- **clientID** には、クライアントの ID 番号が表示されます。
- **clientSeq** には、クライアントの通知シーケンス番号が表示されます。
- 現在の冗長ファシリティの状態。

次の例では、冗長ファシリティカウンタ情報を表示する方法を示します。

```
Device# show redundancy counters

Redundancy Facility OMs
    comm link up = 0
    comm link down = 0

    invalid client tx = 0
    null tx by client = 0
    tx failures = 0
    tx msg length invalid = 0

    client not rxing msgs = 0
    rx peer msg routing errors = 0
    null peer msg rx = 0
    errored peer msg rx = 0

    buffers tx = 135884
    tx buffers unavailable = 0
    buffers rx = 135109
    buffer release errors = 0

    duplicate client registers = 0
    failed to register client = 0
    Invalid client syncs = 0
```

Device#

次の例では、冗長ファシリティ履歴情報を表示する方法を示します。

```
Device# show redundancy history

00:00:04 client added: Redundancy Mode RF(29) seq=60
00:00:04 client added: IfIndex(139) seq=62
00:00:04 client added: CHKPT RF(25) seq=71
00:00:04 client added: QEMU Platform RF(10001) seq=85
00:00:04 client added: Event Manager(77) seq=87
00:00:04 client added: RP Platform RF(1340) seq=104
00:00:04 client added: CWAN HA(1501) seq=105
00:00:04 client added: Network RF Client(22) seq=112
00:00:04 client added: IOSXE SPA TSM(1505) seq=120
00:00:04 client added: LAN-Switch VTP VLAN(501) seq=137
00:00:04 client added: XDR RRP RF Client(71) seq=139
00:00:04 client added: CEF RRP RF Client(24) seq=140
00:00:04 client added: MFIB RRP RF Client(306) seq=150
00:00:04 client added: RFS RF(520) seq=163
00:00:04 client added: klib(33014) seq=167
00:00:04 client added: Config Sync RF client(5) seq=168
00:00:04 client added: NGWC FEC Rf client(10007) seq=173
00:00:04 client added: LAN-Switch Port Manager(502) seq=190
00:00:04 client added: Access Tunnel(530) seq=192
```

show redundancy

```
00:00:04 client added: Mac address Table Manager(519) seq=193
00:00:04 client added: DHCP(100) seq=238
00:00:04 client added: DHCPD(101) seq=239
00:00:04 client added: SNMP RF Client(34) seq=251
00:00:04 client added: CWAN APS HA RF Client(1502) seq=252
00:00:04 client added: History RF Client(35) seq=261
```

<output truncated>

次の例では、冗長ファシリティの状態に関する情報を表示する方法を示します。

```
Device# show redundancy states

    my state = 13 -ACTIVE
    peer state = 8  -STANDBY HOT
        Mode = Duplex
        Unit = Primary
        Unit ID = 5

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State                = sso
    Maintenance Mode = Disabled
    Manual Swact = enabled
    Communications = Up

    client count = 115
    client_notification_TMR = 30000 milliseconds
        RF debug mask = 0x0

Device#
```

show redundancy config-sync

コンフィギュレーション同期障害情報または無視された Mismatched Command List (MCL) (存在する場合) を表示するには、EXEC モードで **show redundancy config-sync** コマンドを使用します。

show redundancy config-sync {failures {bem|mcl|prc}|ignored failures mcl}

Syntax Description	failures	MCL エントリまたはベスト エフォート方式 (BEM) /パーサー リターンコード (PRC) の障害を表示します。
	bem	BEM 障害コマンドリストを表示し、スタンバイを強制的にリポートします。
	mcl	スイッチの実行コンフィギュレーションに存在するがスタンバイのイメージでサポートされていないコマンドを表示し、スタンバイを強制的にリポートします。
	prc	PRC 障害コマンドリストを表示し、スタンバイを強制的にリポートします。
	ignored failures mcl	無視された MCL 障害を表示します。

Command Default なし

Command Modes ユーザ EXEC
特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 2つのバージョンの Cisco IOS イメージが含まれている場合は、それぞれのイメージによってサポートされるコマンドセットが異なる可能性があります。このような不一致コマンドのいずれかがアクティブで実行された場合、スタンバイでそのコマンドを認識できない可能性があり、これにより設定の不一致状態が発生します。バルク同期中にスタンバイでコマンドの構文チェックが失敗すると、コマンドはMCLに移動し、スタンバイはリセットされます。すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブの実行コンフィギュレーションから、不一致コマンドをすべて削除します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイをリロードします。

または、次の手順を実行して MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイをリロードします。システムは SSO モードに遷移します。



Note 不一致コマンドを無視する場合、アクティブとスタンバイの同期していないコンフィギュレーションは存在したままです。

3. 無視された MCL は、**show redundancy config-sync ignored mcl** コマンドを使用して確認できます。

各コマンドでは、そのコマンドを実装するアクション機能において戻りコードが設定されます。この戻りコードは、コマンドが正常に実行されたかどうかを示します。アクティブは、コマンドの実行後に PRC を維持します。スタンバイはコマンドを実行し、アクティブに PRC を返します。これら2つの PRC が一致しないと、PRC 障害が発生します。バルク同期または1行ごとの (LBL) 同期中にスタンバイで PRC エラーが生じた場合、スタンバイはリセットされます。すべての PRC 障害を表示するには、**show redundancy config-sync failures prc** コマンドを使用します。

ベストエフォート方式 (BEM) エラーを表示するには、**show redundancy config-sync failures bem** コマンドを使用します。

次に、BEM 障害を表示する例を示します。

```
Device> show redundancy config-sync failures bem
BEM Failed Command List
-----

The list is Empty
```

次に、MCL 障害を表示する例を示します。

```
Device> show redundancy config-sync failures mcl
Mismatched Command List
-----

The list is Empty
```

次に、PRC 障害を表示する例を示します。

```
Device# show redundancy config-sync failures prc
PRC Failed Command List
-----

The list is Empty
```

show switch

スタックメンバまたはスイッチスタックに関連した情報を表示するには、EXEC モードで **show switch** コマンドを使用します。

show switch [*stack-member-number* | **detail** | **neighbors** | **stack-ports** [**summary**]][**detail**]

Syntax Description		
<i>stack-member-number</i>		(任意) スタック メンバ数。指定できる範囲は 1 ~ 9 です。
detail		(任意) スタック リングの詳細情報を表示します。
neighbors		(任意) スイッチスタック全体のネイバーを表示します。
stack-ports		(任意) スイッチスタック全体のポート情報を表示します。
summary		(任意) スタック ケーブルの長さ、スタック リングのステータス、およびループバックのステータスを表示します。
stack-ports detail		(任意) 各スタックメンバのスタック リングステータス、エラー、ドロップ、送受信されたパケットの総数、伝送レート、スタック リングの帯域幅、および速度を表示します。

Command Default なし

Command Modes ユーザ EXEC
特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.1	detail キーワードが show switch stack-ports detail コマンドに追加されました。

Usage Guidelines このコマンドでは、次のステートが表示されます。

- **Initializing:** スイッチはスタックに追加されたばかりで、ready 状態になるための基本的な初期化が完了していません。
- **HA Sync in Progress:** スタンバイが選出されると、同期が終了するまで対応するスイッチはこの状態のままになります。

- **Syncing:** 既存のスタックに追加されたスイッチは、スイッチ追加シーケンスが完了するまでこの状態のままになります。
- **Ready:** メンバがシステム レベルおよびインターフェイス レベルの設定のロードを完了し、トラフィックを転送できるようになっています。
- **V-Mismatch:** Version-Mismatch モードのスイッチ。Version-Mismatch モードは、スタックに参加したスイッチのソフトウェアバージョンがアクティブスイッチと非互換である場合です。
- **Provisioned:** スイッチ スタックのアクティブ メンバになる前にすでに設定されていたスイッチの状態です。プロビジョニングされたスイッチでは、MAC アドレスおよびプライオリティ番号は、常に 0 と表示されます。
- **Unprovisioned:** プロビジョニングされたスイッチ番号が **no switch switch-number provision** コマンドを使用してプロビジョニング解除された場合の状態です。
- **Removed:** スタックに存在していたスイッチが、**reload slot** コマンドを使用して除外された場合です。
- **Sync not started:** 複数のスイッチが既存のスタックに同時に追加された場合、アクティブスイッチが 1 台ずつ追加します。追加中のスイッチは Syncing 状態になります。まだ追加されていないスイッチは Sync not started 状態になります。
- **Lic-Mismatch:** スイッチのライセンスレベルがアクティブスイッチと異なります。

スタックメンバ（アクティブスイッチを含む）の代表的なステート遷移は、Waiting > Initializing > Ready です。

Version Mismatch (VM) モードのスタックメンバの代表的なステート遷移は、Waiting > Ver Mismatch です。

スイッチスタックにプロビジョニングされたスイッチが存在するかどうかを識別するには、**show switch** コマンドを使用できます。**show running-config** および **show startup-config** 特権 EXEC コマンドでは、この情報は提供されません。

永続的 MAC アドレスがイネーブルになっている場合、スタックの MAC-persistence wait-time も表示されます。

各スタックメンバのスタックリンクに関する詳細情報を表示するには、**show switch stack-ports detail** コマンドを使用します。

Examples

次に、メンバ 6 の要約情報を表示する例を示します。

```
Device# show switch 6
Switch#  Role      Mac Address      Priority    State
-----  -
6         Member      0003.e31a.1e00    1          Ready
```

次に、スタックに関するネイバー情報を表示する例を示します。

```
Device# show switch neighbors
Switch #   Port A      Port B
-----  -

```

```

6      None      8
8      6         None
    
```

次に、スタック ポート情報を表示する例を示します。

```

Device# show switch stack-ports
Switch #   Port A   Port B
-----
6          Down   Ok
8          Ok    Down
    
```

次に、**show switch stack-ports summary** コマンドの出力例を示します。次の表に、この出力で表示されるフィールドについて説明します。

```

Device# show switch stack-ports summary
Switch#/  Stack  Neighbor  Cable  Link  Link  Sync  #      In
Port#     Port   Status    Length OK   Active OK   Changes  Loopback
To LinkOK
-----
1/1      Down   2         50 cm  No   NO   No   10     No
1/2      Ok     3         1 m    Yes  Yes  Yes  0      No
2/1      Ok     5         3 m    Yes  Yes  Yes  0      No
2/2      Down   1         50 cm  No   No   No   10     No
3/1      Ok     1         1 m    Yes  Yes  Yes  0      No
3/2      Ok     5         1 m    Yes  Yes  Yes  0      No
5/1      Ok     3         1 m    Yes  Yes  Yes  0      No
5/2      Ok     2         3 m    Yes  Yes  Yes  0      No
    
```

Table 154: show switch stack-ports summary コマンドの出力

フィールド	説明
Switch#/Port#	メンバー番号と、そのスタックポート番号。
スタックポートのステータス	スタックポートのステータス。 <ul style="list-style-type: none"> • Down: ケーブルは検出されましたが、接続されたネイバーがアップになっていないか、スタックポートがディセーブルになっています。 • OK: ケーブルが検出され、接続済みのネイバーが起動しています。
Neighbor	スタックケーブルの接続先の、アクティブなメンバーのスイッチの数。
ケーブル長	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は <i>no cable</i> になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。

フィールド	説明
リンク OK	<p>スタックケーブルが接続され機能しているかどうか。相手側には、接続されたネイバーが存在する場合も、そうでない場合もあります。</p> <p>リンクパートナーは、ネイバースイッチ上のスタックポートのことです。</p> <ul style="list-style-type: none"> • No: このポートに接続されているスタックケーブルがないか、スタックケーブルが機能していません。 • Yes: このポートには正常に機能するスタックケーブルが接続されています。
リンクアクティブ	<p>スタックケーブル相手側にネイバーが接続されているかどうか。</p> <ul style="list-style-type: none"> • No: 相手側にネイバーが検出されません。ポートは、このリンクからトラフィックを送信できません。 • Yes: 相手側にネイバーが検出されました。ポートは、このリンクからトラフィックを送信できます。
同期 OK	<p>リンクパートナーが、スタックポートに有効なプロトコルメッセージを送信するかどうか。</p> <ul style="list-style-type: none"> • No: リンクパートナーからスタックポートに有効なプロトコルメッセージが送信されません。 • Yes: リンクの相手側は、ポートに有効なプロトコルメッセージを送信します。
# Changes to LinkOK	<p>リンクの相対的安定性。</p> <p>短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。</p>
ループバック内	<p>スタックケーブルがメンバのスタックポートに接続されているかどうか。</p> <ul style="list-style-type: none"> • No: メンバ上の少なくとも1つのスタックポートに接続済みのスタックケーブルがあります。 • Yes: メンバのどのスタックポートにも、スタックケーブルが接続されていません。

次に、**show switch stack-ports detail** コマンドの出力例を示します。

```
Device# show switch stack-ports detail
1/1 is OK Loopback No
Cable Length 50cm      Neighbor 2
Link Ok Yes Sync Ok Yes Link Active Yes
Changes to LinkOK 1
  Five minute input rate 430998 packets/sec
  Five minute output rate 100989 packets/sec
    2198108 packets input, 17584864 bytes
```

```

553113 packets output, 4424904 bytes
CRC Errors
    Data CRC 0
    Ringword CRC 0
    InvRingWord 0
    PcsCodeWord 0
1/2 is OK Loopback No
Cable Length 50cm      Neighbor 3
Link Ok Yes Sync Ok Yes Link Active Yes
Changes to LinkOK 1
Five minute input rate 743042 packets/sec
Five minute output rate 79830 packets/sec
3765816 packets input, 30126528 bytes
439001 packets output, 3512008 bytes
CRC Errors
    Data CRC 0
    Ringword CRC 0
    InvRingWord 0
    PcsCodeWord 0
...
...
...
...

```

Table 155: show switch stack-ports detail コマンドの出力

フィールド	説明
Neighbor	スタックケーブルの接続先の、アクティブなメンバーのスイッチの数。
ケーブル長	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は <i>Unknown</i> になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。
リンク OK	スタックケーブルが接続され機能しているかどうか。相手側には、接続されたネイバーが存在する場合も、そうでない場合もあります。 リンクパートナーは、ネイバースイッチ上のスタックポートのことです。 <ul style="list-style-type: none"> • No: このポートに接続されているスタックケーブルがないか、スタックケーブルが機能していません。 • Yes: このポートには正常に機能するスタックケーブルが接続されています。
リンクアクティブ	スタックケーブル相手側にネイバーが接続されているかどうか。 <ul style="list-style-type: none"> • No: 相手側にネイバーが検出されません。ポートは、このリンクからトラフィックを送信できません。 • Yes: 相手側にネイバーが検出されました。ポートは、このリンクからトラフィックを送信できます。

フィールド	説明
同期 OK	<p>リンクパートナーが、スタックポートに有効なプロトコルメッセージを送信するかどうか。</p> <ul style="list-style-type: none"> • No: リンクパートナーからスタックポートに有効なプロトコルメッセージが送信されません。 • Yes: リンクの相手側は、ポートに有効なプロトコルメッセージを送信します。
# Changes to LinkOK	<p>リンクの相対的安定性。</p> <p>短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。</p>
5 分入力レート	<p>パケットが受信される平均レート（5 分間で計算）。パケット/秒で測定されます。</p>
5 分出力レート	<p>パケットが送信される平均レート（5 分間で計算）。パケット/秒単位で測定されます。</p>
CRC Errors	<p>スタックインターフェイスで見られるさまざまなタイプの巡回冗長検査（CRC）エラー：</p> <ul style="list-style-type: none"> • Data CRC: スタック インターフェイス データ CRC エラー • Ringword CRC: Stack interface ring word CRC エラー • InvRingWord: Stack interface invalid ring word エラー • PcsCodeWord: Stack interface Physical Coding Sublayer（PCS）エラー <p>これらのエラーは通常、スイッチオーバーまたはスイッチのリロードによってスタックインターフェイスの状態が変化したときに発生します。このようなエラーは無視できます。</p> <p>ただし、これらのエラーカウンターが大幅に増加する場合、または一定期間にわたって継続的に増加する場合は、スタックケーブルに問題がないか確認してください。</p> <p>すべてのポートのスタックカウンタをクリアするには、clear counters コマンドを使用します。</p>

show switch stack-mode

デバイスの現在のスタックモードを表示し確認するには、特権 EXEC モードでコマンド **show switch stack-mode** を使用します。

show switch stack-mode

Command Default なし

Command Modes privileged EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Usage Guidelines **show switch stack-mode** コマンドは、現在実行しているスタックモードの詳細なステータスを表示します。スタック内のそれぞれのデバイスに表示されるフィールドには、デバイスのロール、その MAC アドレス、再起動後のスタックモード、現在のスタックモードなどがあります。

```
Device# show switch stack-mode
Switch  Role    Mac Address      Version  Mode    Configured  State
-----  -
1        Member  3c5e.c357.c880   V05     1+1'    Active'     Ready
*2        Active  547c.69de.cd00   V05     1+1'    Standby'    Ready
3        Member  547c.6965.cf80   V05     1+1'    Member'     Ready
```

Mode フィールドには、現在のスタック モードが表示されます。

Configured フィールドは、再起動後に想定されるデバイス状態を参照します。

単一引用符 (') は、スタック モードが変更されていることを示します。

stack-mac persistent timer

固定MAC アドレス機能を有効にするには、スイッチスタックまたはスタンドアロンスイッチのグローバル コンフィギュレーション モードで **stack-mac persistent timer** コマンドを使用します。固定 MAC アドレス機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

stack-mac persistent timer [*0time-value*]

no stack-mac persistent timer

Syntax Description

0 (任意) 現在のスタックのアクティブスイッチの MAC アドレスの使用を継続し、新しいアクティブスイッチが引き継いだ場合もそうします。

time-value (任意) スタック MAC アドレスが新しいアクティブの MAC アドレスに変わるまでの時間 (分単位)。指定できる範囲は 1 ~ 60 分です。

Command Default

固定 MAC アドレスはディセーブルに設定されています。スタックの MAC アドレスは、常に最初のアクティブスイッチの MAC アドレスです。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

デフォルトでは、新しいアクティブ スイッチが引き継ぐ場合でも、スタック MAC アドレスは最初のアクティブスイッチの MAC アドレスになります。 **stack-mac persistent timer** コマンドまたは **stack-mac persistent timer 0** コマンドを入力すると、同じ動作が発生します。



Note PAgP フラップを回避するには、**stack-mac persistent timer 0** を使用してスタック MAC 永続待機タイマーを無期限に設定する必要があります。

stack-mac persistent timer コマンドを *time-value* とともに入力すると、新しいスイッチがアクティブスイッチになったときに、入力した時間の後にスタック MAC アドレスが新しいアクティブスイッチのものに変わります。以前のアクティブスイッチがこの時間内にスタックに再加入した場合、スタックはその MAC アドレスを持つスイッチがスタック内に存在する限り、その MAC アドレスを保持します。

スタック全体をリロードすると、アクティブ スイッチの MAC アドレスがスタックの MAC アドレスになります。



Note スタック MAC アドレスを変更しない場合、レイヤ 3 インターフェイスのフラップが発生しません。これは、未知の MAC アドレス（スタック内のスイッチに属さない MAC アドレス）がスタック MAC アドレスになる可能性があることを意味します。この未知の MAC アドレスを持つスイッチが別のスタックにアクティブスイッチとして参加すると、2つのスタックが同じスタック MAC アドレスを持つこととなります。**stack-mac update force** コマンドを使用して、この競合を解決する必要があります。

Examples

次に、固定 MAC アドレスをイネーブルにする例を示します。

```
Device(config)# stack-mac persistent timer
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。イネーブルの場合、出力に **stack-mac persistent timer** が表示されます。

stack-mac update force

スタック MAC アドレスをアクティブスイッチの MAC アドレスに更新するには、アクティブスイッチの EXEC モードで **stack-mac update force** コマンドを使用します。

stack-mac update force

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes ユーザ EXEC

特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines デフォルトでは、ハイアベイラビリティ (HA) フェールオーバー時に、スタックの MAC アドレスは新しいアクティブスイッチの MAC アドレスに変更されません。スタック MAC アドレスが新しいアクティブスイッチの MAC アドレスに強制的に変更されるようにするには、**stack-mac update force** コマンドを使用します。

スタック MAC アドレスと同じ MAC アドレスを持つスイッチが現在そのスタックのメンバである場合、**stack-mac update force** コマンドは無効です (スタック MAC アドレスはアクティブスイッチの MAC アドレスに更新されません)。



Note スタック MAC アドレスを変更しない場合、レイヤ 3 インターフェイスのフラップが発生しません。これは、未知の MAC アドレス (スタック内のスイッチに属さない MAC アドレス) がスタック MAC アドレスになる可能性があることを意味します。この未知の MAC アドレスを持つスイッチが別のスタックにアクティブスイッチとして参加すると、2つのスタックが同じスタック MAC アドレスを持つこととなります。**stack-mac update force** コマンドを使用して、この競合を解決する必要があります。

次に、スタック MAC アドレスをアクティブスイッチの MAC アドレスに更新する例を示します。

```
デバイス> stack-mac update force
デバイス>
```

設定を確認するには、**show switch** 特権 EXEC コマンドを入力します。スタック MAC アドレスには、MAC アドレスがローカルと未知のどちらであるかも含まれます。

standby console enable

スタンバイ コンソールへのアクセスをイネーブルにするには、冗長メインコンフィギュレーションサブモードで **standby console enable** コマンドを使用します。スタンバイ コンソール へのアクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

standby console enable
no standby console enable

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

スタンバイ コンソール へのアクセスはディセーブルです。

Command Modes

冗長メイン コンフィギュレーション サブモード

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

このコマンドは、スタンバイ コンソールに関する特定のデータを収集し、確認するために使用されます。コマンドは、主にシスコのテクニカルサポート担当がのトラブルシューティングを行うのに役立ちます。

次に、冗長メインコンフィギュレーションサブモードを開始し、スタンバイ コンソールへのアクセスをイネーブルにする例を示します。

```
Device(config)# redundancy  
Device(config-red)# main-cpu  
Device(config-r-mc)# standby console enable  
Device(config-r-mc)#
```

switch clear stack-mode

スタックモードを N+1 に変更して、アクティブおよびスタンバイの 1: 1 モードの割り当てを削除するには、特権 EXEC モードで **switch clear stack-mode** コマンドを使用します。

switch clear stack-mode

Command Default なし

Command Modes privileged EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Usage Guidelines 1: 1 の冗長モードをディセーブルにし、スタックを N+1 モードに設定するには、このコマンドを使用します。

```
Device> enable
Device# switch clear stack-mode
WARNING: Clearing the chassis HA configuration will result in the chassis coming up in Stand
Alone mode after reboot.The HA configuration will remain the same on other chassis. Do you
wish to continue? [y/n]? [yes]:
```

switch switch-number role

スタック内のデバイスのロールをアクティブまたはスタンバイのいずれかに変更するには、特権 EXEC モードで **switch switch-numberrole** コマンドを使用します。

switch switch-number role {standby | active}

Syntax Description

Syntax Description	switch-number	スタック メンバの番号です。
	standby	デバイスをスタックのスタンバイデバイスとして指定します。
	active	デバイスをスタックのアクティブなデバイスとして指定します。

Command Default

なし

Command Modes

privileged EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

Usage Guidelines

デバイスをスタック内のアクティブロールまたはスタンバイロールに設定するには、このコマンドを使用します。スタック内の他のデバイスはスタックのメンバのまま残ります。



Note デバイスのロールを変更すると、冗長モードがスタックに対して 1: 1 のモードに設定されます。設定されたアクティブまたはスタンバイ デバイスが起動しない場合、スタックは起動することができません。

次に、デバイス 2 をアクティブなデバイスに、デバイス 1 をスタックのスタンバイ デバイスに設定する例を示します。

```
Device> enable
Device# switch 2 role active
WARNING: Changing the switch role may result in redundancy mode being configured to 1+1 mode for this stack. If the configured Active or Standby switch numbers do not boot up, then the stack will not be able to boot. Do you want to continue?[y/n]? : yes
```

```
Device# switch 1 role standby
WARNING: Changing the switch role may result in redundancy mode being configured to 1+1 mode for this stack. If the configured Active or Standby switch numbers do not boot up, then the stack will not be able to boot. Do you want to continue?[y/n]? : yes
```

switch stack port

メンバの指定されたスタックポートをディセーブルまたはイネーブルにするには、スタックメンバの特権 EXEC モードで **switch** コマンドを使用します。

switch *stack-member-number* **stack port** *port-number* {**disable** | **enable**}

Syntax Description

stack-member-number 現在のスタック メンバ番号。指定できる範囲は 1～8 です。

stack port *port-number* メンバ上のスタック ポートを指定します。指定できる範囲は 1～2 です。

disable 指定したポートをディセーブルにします。

enable 指定されたポートをイネーブルにします。

Command Default

スタック ポートはイネーブルです。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スタックが次の状態 スタックが **full-ring** 状態になるのは、すべてのスタック メンバがスタックポートを使用して接続され、**ready** 状態になっている場合です。

スタックが次の状態 スタックが **partial-ring** 状態になるのは、次が発生したときです。

- すべてのメンバがスタック ポートを通じて接続されたが、一部が **ready** ステートではない。
- スタック ポートを通じて接続されていないメンバーがある。



Note

switch *stack-member-number* **stack port** *port-number* **disable** コマンドを使用するときは注意してください。スタック ポートをディセーブルにすると、スタックは半分の帯域幅で稼働します。

switch *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力し、スタックが **full-ring** 状態にある場合、ディセーブルにできるスタックポートは1つだけです。次のメッセージが表示されます。

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

switch *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力し、スタックが **partial-ring** 状態にある場合、ポートはディセーブルにできません。次のメッセージが表示されます。

```
Disabling stack port not allowed with current stack configuration.
```

Examples

次に、member 4 上の stack port 2 をディセーブルにする方法の例を示します。

```
デバイス# switch 4 stack port 2 disable
```

switch priority

値をのプライオリティ値を変更するには、アクティブスイッチの EXEC モードで **switch priority** コマンドを使用します。

switch *stack-member-number* **priority** *new-priority-value*

Syntax Description	<i>stack-member-number</i> 現在のスタック メンバ番号。指定できる範囲は 1～8 です。
	<i>new-priority-value</i> スタック メンバの新しいプライオリティ値指定できる範囲は 1～15 です。
Command Default	デフォルトのプライオリティ値は 1 です。
Command Modes	ユーザ EXEC 特権 EXEC
Command History	リリース 変更内容 Cisco IOS XE Fuji 16.9.2 このコマンドが導入されました。

Usage Guidelines 新しいプライオリティ値は、新しいアクティブスイッチ選定の要素になります。プライオリティ値を変更しても、アクティブスイッチがただちに変更されることはありません。

Examples

次の例では、スタック メンバ 6 のプライオリティ値を 8 に変更する方法を示します。

```
デバイス# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

switch provision

新しいスイッチがスイッチスタックに追加される前に構成設定するには、アクティブスイッチのグローバル コンフィギュレーション モードで **switch provision** コマンドを使用します。除外されたスイッチ（スタックを離れたスタック メンバ）に対応するすべての設定情報を削除するには、このコマンドの **no** 形式を使用します。

switch stack-member-number provision type
no switch stack-member-number provision

Syntax Description

stack-member-number スタック メンバの番号です。指定できる範囲は 1～8 です。

type 新しいスイッチがスタックに加入する前の、このスイッチのタイプ。

Command Default

スイッチは、プロビジョニングされていません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

type には、コマンドライン ヘルプ スtring に示されたサポート対象のスイッチのモデル番号を入力します。

エラー メッセージを受信しないようにするには、このコマンドの **no** 形式を使用してプロビジョニングされた設定を削除する前に、スイッチスタックから指定のスイッチを削除する必要があります。

スイッチタイプを変更する場合も、スイッチスタックから指定のスイッチを削除する必要があります。スイッチタイプを変更しない場合でも、スイッチスタック内に物理的に存在するプロビジョニングされたスイッチのスタック メンバ番号を変更できます。

プロビジョニングされたスイッチのタイプが、スタック上のプロビジョニングされた設定のスイッチタイプと一致しない場合、スイッチスタックはプロビジョニングされたスイッチにデフォルト設定を適用し、これをスタックに追加します。スイッチスタックでは、デフォルト設定を適用する場合にメッセージを表示します。

プロビジョニング情報は、スイッチスタックの実行コンフィギュレーションで表示されます。

copy running-config startup-config 特権 EXEC コマンドを入力すると、プロビジョニングされた設定がスイッチスタックのスタートアップコンフィギュレーション ファイルに保存されます。



Caution **switch provision** コマンドを使用すると、プロビジョニングされた設定にメモリが割り当てられます。新しいスイッチタイプが設定されたときに、以前割り当てられたメモリのすべてが解放されるわけではありません。そのため、このコマンドをおおよそ 200 回を超えて使用しないようにしてください。スイッチのメモリが不足し、予期せぬ動作が発生する可能性があります。

Examples

次に、スタック メンバー番号 2 が設定されたスイッチをスイッチ スタックに割り当てる例を示します。**show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
デバイス(config)# switch 2 provision WS-xxxx
デバイス(config)# end
デバイス# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

また、**show switch** ユーザ EXEC コマンドを入力すると、スイッチ スタックのプロビジョニングされたステータスを表示できます。

次の例では、スイッチがスタックから削除される場合に、スタック メンバ 5 についてのすべての設定情報が削除される方法を示します。

```
デバイス(config)# no switch 5 provision
```

プロビジョニングされたスイッチが、実行コンフィギュレーションで追加または削除されたことを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

switch renumber

スタックメンバ番号を変更するには、アクティブスイッチの EXEC モードで **switch renumber** コマンドを使用します。

```
switch current-stack-member-number renumber new-stack-member-number
```

Syntax Description

current-stack-member-number 現在のスタックメンバ番号。指定できる範囲は 1～8 です。

new-stack-member-number スタックメンバの新しいスタックメンバ番号。指定できる範囲は 1～8 です。

Command Default

デフォルトのスタックメンバ番号は 1 です。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

指定したメンバ番号をすでに他のスタックメンバが使用している場合、スタックメンバをリロードする際にアクティブスイッチは使用可能な一番低い番号を割り当てます。



Note スタックメンバ番号を変更し、新しいスタックメンバ番号がどの設定にも関連付けされていない場合、そのスタックメンバは現在の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。

プロビジョニングされたスイッチでは、**switch current-stack-member-number renumber new-stack-member-number** コマンドを使用しないでください。使用すると、コマンドは拒否されません。

スタックメンバをリロードし、設定変更を適用するには、**reload slot current stack member number** 特権 EXEC コマンドを使用します。

Examples

次の例では、スタックメンバ 6 のメンバ番号を 7 に変更する方法を示しています。

```
デバイス# switch 6 renumber 7
```

```
WARNING:Changing the switch number may result in a configuration change for that switch.  
The interface configuration associated with the old switch number will remain as a provisioned  
configuration.
```

```
Do you want to continue?[confirm]
```

switch renumber

スタックメンバ番号を変更するには、アクティブスイッチの EXEC モードで **switch renumber** コマンドを使用します。

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

current-stack-member-number 現在のスタック メンバ番号。指定できる範囲は 1～8 です。

new-stack-member-number スタック メンバの新しいスタック メンバ番号。指定できる範囲は 1～8 です。

Command Default

デフォルトのスタック メンバ番号は 1 です。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

指定したメンバ番号をすでに他のスタックメンバが使用している場合、スタックメンバをリロードする際に アクティブスイッチ は使用可能な一番低い番号を割り当てます。



Note スタックメンバ番号を変更し、新しいスタックメンバ番号がどの設定にも関連付けされていない場合、そのスタックメンバは現在の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。

プロビジョニングされたスイッチでは、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* コマンドを使用しないでください。使用すると、コマンドは拒否されます。

スタックメンバをリロードし、設定変更を適用するには、**reload slot** *current stack member number* 特権 EXEC コマンドを使用します。

Examples

次の例では、スタックメンバ 6 のメンバ番号を 7 に変更する方法を示しています。

```

デバイス# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
configuration.
Do you want to continue?[confirm]
```



PART **XII**

システム管理

- システム管理コマンド, on page 1693
- トレース, on page 1941



システム管理コマンド

- [arp](#), on page 1696
- [boot](#), on page 1697
- [boot system](#), on page 1698
- [cat](#), on page 1699
- [copy](#), on page 1700
- [copy startup-config tftp:](#), on page 1701
- [copy tftp: startup-config](#), on page 1702
- [debug voice diagnostics mac-address](#), on page 1703
- [debug platform condition feature multicast controlplane](#), on page 1704
- [debug platform condition mac](#), on page 1706
- [debug platform rep](#), on page 1708
- [debug ilpower powerman](#), on page 1710
- [delete](#), on page 1713
- [dir](#), on page 1714
- [exit](#), on page 1716
- [factory-reset](#), on page 1717
- [flash_init](#), on page 1720
- [help](#), on page 1721
- [hostname](#), on page 1722
- [install](#), on page 1724
- [ip http banner](#), on page 1738
- [ip http banner-path](#), on page 1739
- [ip ssh bulk-mode](#), on page 1740
- [l2 traceroute](#), on page 1741
- [license air level](#), on page 1742
- [license boot level](#), on page 1744
- [license smart \(グローバル コンフィギュレーション\)](#), on page 1747
- [license smart \(特権 EXEC\)](#), on page 1758
- [license smart deregister](#), on page 1764
- [license smart register idtoken](#), on page 1766
- [license smart renew](#), on page 1768
- [location](#), on page 1770
- [location plm calibrating](#), on page 1774

- `mgmt_init`, on page 1775
- `mkdir`, on page 1776
- `more`, on page 1777
- `no debug all`, on page 1778
- `rename`, on page 1779
- `request consent-token accept-response shell-access`, on page 1780
- `request consent-token generate-challenge shell-access`, on page 1781
- `request consent-token terminate-auth`, on page 1782
- `request platform software console attach switch`, on page 1783
- `reset`, on page 1785
- `rmdir`, on page 1786
- `sdm prefer`, on page 1787
- `service private-config-encryption`, on page 1788
- `set`, on page 1789
- `show avc client`, on page 1792
- `show bootflash:`, on page 1793
- `show debug`, on page 1796
- `show env xps`, on page 1797
- `show flow monitor`, on page 1801
- `show install`, on page 1806
- `show location`, on page 1808
- `show logging onboard switch uptime`, on page 1810
- `show license all`, on page 1813
- `show license authorization`, on page 1818
- `show license data translation`, on page 1823
- `show license eventlog`, on page 1824
- `show license history message`, on page 1826
- `show license reservation`, on page 1827
- `show license status`, on page 1828
- `show license summary`, on page 1837
- `show license tech`, on page 1840
- `show license udi`, on page 1848
- `show license usage`, on page 1850
- `show mac address-table`, on page 1854
- `show mac address-table move update`, on page 1859
- `show parser encrypt file status`, on page 1860
- `show platform integrity`, on page 1861
- `show platform software audit`, on page 1862
- `show platform software fed switch punt cause`, on page 1866
- `show platform software fed switch punt cpuq`, on page 1868
- `show platform software sl-infra`, on page 1871
- `show platform sudi certificate`, on page 1872
- `show running-config`, on page 1874
- `show sdm prefer`, on page 1880
- `show tech-support confidential`, on page 1882
- `show tech-support license`, on page 1883

- [show tech-support monitor](#), on page 1885
- [show tech-support platform](#), on page 1886
- [show tech-support platform evpn_vxlan](#), on page 1890
- [show tech-support platform fabric](#), on page 1893
- [show tech-support platform igmp_snooping](#), on page 1897
- [show tech-support platform layer3](#), on page 1900
- [show tech-support platform mld_snooping](#), on page 1908
- [show tech-support port](#), on page 1915
- [show tech-support pvlan](#), on page 1918
- [show version](#), on page 1919
- [system env temperature threshold yellow](#), on page 1927
- [tftp-server](#), on page 1929
- [traceroute mac](#), on page 1931
- [traceroute mac ip](#), on page 1934
- [type](#), on page 1937
- [unset](#), on page 1938
- [version](#), on page 1940

arp

Address Resolution Protocol (ARP) テーブルの内容を表示するには、ブートローダモードで **arp** コマンドを使用します。

arp [*ip_address*]

Syntax Description *ip_address* (任意) ARP テーブルまたは特定の IP アドレスのマッピングを表示します。

Command Default デフォルトの動作や値はありません。

Command Modes ブートローダ

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ARP テーブルには、IP アドレスと MAC アドレスのマッピングが示されます。

Examples 次に、ARP テーブルを表示する例を示します。

```
Device: arp 172.20.136.8  
arp'ing 172.20.136.8...  
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

実行可能イメージをロードおよびブートして、コマンドライン インターフェイス (CLI) を表示するには、ブートローダモードで **boot** コマンドを使用します。

boot *flag* *filesystem:/file-url...*

Syntax Description	
<i>filesystem:</i>	ファイルシステムのエイリアス。システムボードフラッシュデバイスには flash: を使用します。USB メモリスティックには usbflash0: を使用します。
<i>/file-url</i>	ブート可能なイメージのパス (ディレクトリ) および名前。各イメージ名はセミコロンで区切ります。

Command Default デフォルトの動作や値はありません。

Command Modes ブートローダ

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines 引数を何も指定しないで **boot** コマンドを入力した場合、デバイスは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的にブートしようとします。

file-url 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージをブートしようとします。

ブートローダ **boot** コマンドのオプションを設定した場合は、このコマンドがただちに実行され、現在のブートローダセッションだけに適用されます。

これらの設定が保存されて次回のブート処理に使用されることはありません。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

例

次の例では、*new-image.bin* イメージを使用してデバイスをブートする方法を示します。

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

このコマンドを入力すると、セットアッププログラムを開始するように求められます。

boot system

次回のブートサイクル中にロードするシステムイメージを指定するには、グローバル コンフィギュレーション モードで **boot system** コマンドを使用します。起動システムイメージの指定を削除するには、このコマンドの **no** 形式を使用します。

```
boot system {filesystem: /file-url | switch all filesystem: /file-url}
no boot system [filesystem: /file-url | switch all [filesystem: /file-url]]
```

Syntax Description

filesystem: ファイルシステムを指定します。オプションは *bootflash:*、*flash:*、*ftp:*、*http:*、*sftp:*、および *tftp:* です。

switch all スタック内のすべてのデバイスのシステムイメージを設定します。

/file-url システムの起動時にロードするシステムイメージの URL です。

Command Default

デフォルトの動作や値はありません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、ブートフラッシュから `cat9k_lite_iosxe.16.09.03.SPA.bin` という名前のシステムイメージファイルをブートする例を示します。

```
Device(config)# boot system bootflash:cat9k_lite_iosxe.16.09.03.SPA.bin
```

次に、IP アドレスを持つネットワークサーバからスタック内のすべてのデバイスをブートする例を示します。

```
Device(config)# boot system switch all tftp://10.11.15.10/cat9k_lite_iosxe.16.09.03.SPA.bin
```

cat

1 つ以上のファイルの内容を表示するには、ブートローダモードで **cat** コマンドを使用します。

cat *filesystem:/file-url...*

Syntax Description

filesystem: ファイルシステムを指定します。

/file-url 表示するファイルのパス（ディレクトリ）と名前を指定します。ファイル名はスペースで区切ります。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

Examples

次の例では、イメージファイルの内容を表示する方法を示します。

```
Device: cat flash: image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

copy

ファイルをコピー元からコピー先にコピーするには、ブートローダモードで **copy** コマンドを使用します。

copy *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem: ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

/source-file-url コピー元のパス（ディレクトリ）およびファイル名です。

/destination-file-url コピー先のパス（ディレクトリ）およびファイル名です。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 127 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

ファイルを別のディレクトリにコピーする場合は、そのディレクトリが存在していなければなりません。

Examples

次の例では、ルートにあるファイルをコピーする方法を示します。

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

ファイルがコピーされたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

copy startup-config tftp:

スイッチから TFTP サーバに設定をコピーするには、特権 EXEC モードで **copy startup-config tftp:** コマンドを使用します。

copy startup-config tftp: *remote host {ip-address}/{name}*

Syntax Description

remote host {ip-address}/{name} リモートホストのホスト名または IP アドレス。

Command Default

デフォルトの動作や値はありません。

Command Modes

特権 EXEC

Command History

リリース	変更内容
------	------

Cisco IOS XE リリース 16.1 このコマンドが導入されました。

Usage Guidelines

スイッチから現在の設定をコピーするには、**copy startup-config tftp:** コマンドを実行し、続く指示に従います。設定が TFTP サーバにコピーされます。

次に、別のスイッチへログインし、**copy tftp: startup-config** コマンドを実行して、続く指示に従います。これで、設定は別のスイッチにコピーされます。

Examples

次に、TFTP サーバに設定をコピーする例を示します。

```
Device: copy startup-config tftp:  
Address or name of remote host []?
```

copy tftp: startup-config

TFTPサーバから新しいスイッチに設定をコピーするには、新しいスイッチ上で、特権 EXEC モードで **copy tftp: startup-config** コマンドを使用します。

```
copy tftp: startup-config remote host {ip-address}/{name}
```

Syntax Description	<i>remote host {ip-address}/{name}</i> リモートホストのホスト名またはIPアドレス。
---------------------------	---

Command Default	デフォルトの動作や値はありません。
------------------------	-------------------

Command Modes	特権 EXEC
----------------------	---------

Command History	リリース	変更内容
	Cisco IOS XE リリース 16.1	このコマンドが導入されました。

Usage Guidelines	設定をコピーした後、その設定を保存するには、 write memory コマンドを使用し、その後スイッチをリロードするか、または copy startup-config running-config コマンドを実行します。
-------------------------	---

Examples	次に、TFTP サーバからスイッチに設定をコピーする例を示します。
-----------------	-----------------------------------

```
Device: copy tftp: startup-config  
Address or name of remote host []?
```

debug voice diagnostics mac-address

音声クライアントの音声診断のデバッグを有効にするには、特権 EXEC モードで **debug voice diagnostics mac-address** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug voice diagnostics mac-address mac-address1 verbose mac-address mac-address2 verbose
nodebug voice diagnostics mac-address mac-address1 verbose mac-address mac-address2 verbose

Syntax Description	voice diagnostics	音声クライアントの音声のデバッグを設定します。				
	mac-address mac-address1 mac-address mac-address2	音声クライアントの MAC アドレスを指定します。				
	verbose	音声診断の冗長モードを有効にします。				
Command Default	デフォルトの動作や値はありません。					
Command Modes	特権 EXEC					
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE Fuji 16.9.2</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。	
リリース	変更内容					
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。					

以下は、**debug voice diagnostics mac-address** コマンドの出力例で、MAC アドレスが 00:1f:ca:cf:b6:60 である音声クライアントの音声診断のデバッグを有効にする手順を示しています。

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

debug platform condition feature multicast controlplane

Internet Group Management Protocol (IGMP) およびマルチキャストリスナー検出 (MLD) のスヌーピング機能の放射線トレースを有効にするには、特権 EXEC モードで **debug platform condition feature multicast controlplane** コマンドを使用します。放射線トレースを無効にするには、このコマンドの **no** 形式を使用します。

```
debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {ipv4 address / ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address / ipv6 address} vlan vlan-id } level {debug | error | info | verbose | warning}
no debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {ipv4 address / ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address / ipv6 address} vlan vlan-id } level {debug | error | info | verbose | warning}
```

Syntax Description		
	igmp-debug	IGMP 制御の放射線トレースを有効にします。
	pim	Protocol Independent Multicast (PIM) 制御の放射線トレースを有効にします。
	mld-snooping	MLD スヌーピング制御の放射線トレースを有効にします。
	igmp-snooping	IGMP スヌーピング制御の放射線トレースを有効にします。
	mac mac-address	受信者の MAC アドレス。
	group-ip {ipv4 address / ipv6 address}	igmp-debug または pim グループの IPv4 または IPv6 アドレス。
	ip {ipv4 address / ipv6 address}	mld-snooping または igmp-snooping グループの IPv4 または IPv6 アドレス。
	vlan vlan-id	VLAN ID。指定できる範囲は 1 ～ 4094 です。
	level	デバッグの重大度レベルを有効にします。
	debug	デバッグレベルを有効にします。
	error	エラーデバッグを有効にします。

info	情報デバッグを有効化します。
verbose	詳細デバッグを有効にします。
warning	警告デバッグを有効にします。

Command Modes 特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、IGMP スヌーピングの放射線トレース有効にする例を示します。

```
Device# debug platform condition feature multicast controlplane igmp-snooping mac
000a.f330.344a ip 10.1.1.10 vlan 550 level warning
```

Related Commands	Command	Description
	clear debug platform condition all	プラットフォームに適用されているデバッグ条件を削除します。
	debug platform condition	指定した条件に基づいて debug コマンドのデバッグ出力をフィルタリングします。
	debug platform condition start	システムの条件付きデバッグを開始します。
	debug platform condition stop	システムの条件付きデバッグを停止します。
	show platform condition	現在アクティブなデバッグ設定を表示します。

debug platform condition mac

MAC ラーニングの放射線トレースを有効にするには、特権 EXEC モードで **debug platform condition mac** コマンドを使用します。MAC ラーニングの放射線トレースを無効にするには、このコマンドの **no** 形式を使用します。

debug platform condition mac {*mac-address* {**control-plane** | **egress** | **ingress**} | **access-list** *access-list name* {**egress** | **ingress**}}

no debug platform condition mac {*mac-address* {**control-plane** | **egress** | **ingress**} | **access-list** *access-list name* {**egress** | **ingress**}}

Syntax Description

mac <i>mac-address</i>	指定された MAC アドレスに基づいて出力をフィルタリングします。
access-list <i>access-list name</i>	指定されたアクセスリストに基づいて出力をフィルタリングします。
control-plane	コントロールプレーンのルーチンに関するメッセージを表示します。
egress	発信パケットに基づいて出力をフィルタリングします。
ingress	着信パケットに基づいて出力をフィルタリングします。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、MAC アドレスに基づいてデバッグ出力をフィルタリングする例を示します。

```
Device# debug platform condition mac bc16.6509.3314 ingress
```

Related Commands

Command	Description
show platform condition	現在アクティブなデバッグ設定を表示します。
debug platform condition	指定した条件に基づいて debug コマンドのデバッグ出力をフィルタリングします。

Command	Description
debug platform condition start	システムの条件付きデバッグを開始します。
debug platform condition stop	システムの条件付きデバッグを停止します。
clear debug platform condition all	プラットフォームに適用されているデバッグ条件を削除します。

debug platform rep

Resilient Ethernet Protocol (REP) 機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug platform rep** コマンドを使用します。指定した条件を削除するには、このコマンドの **no** 形式を使用します。

```
debug platform rep {all | error | event | packet | verbose}
no debug platform rep {all | error | event | packet | verbose}
```

Syntax Description		
	all	すべての REP デバッグ機能をイネーブルにします。
	error	REP エラーデバッグをイネーブルにします。
	event	REP イベントデバッグをイネーブルにします。
	packet	REP パケットデバッグをイネーブルにします。
	verbose	REP 詳細デバッグをイネーブルにします。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、すべての機能のデバッグをイネーブルにする例を示します。

```
Device# debug platform rep all

debug platform rep verbose debugging is on
debug platform rep control pkt handle debugging is on
debug platform rep error debugging is on
debug platform rep event debugging is on
```

Related Commands

Command	Description
show platform condition	現在アクティブなデバッグ設定を表示します。
debug platform condition	指定した条件に基づいて debug コマンドのデバッグ出力をフィルタリングします。

Command	Description
debug platform condition start	システムの条件付きデバッグを開始します。
debug platform condition stop	システムの条件付きデバッグを停止します。
clear debug platform condition all	プラットフォームに適用されているデバッグ条件を削除します。

debug ilpower powerman

電源コントローラおよびPower over Ethernet (PoE) システムのデバッグをイネーブルにするには、特権 EXEC モードで **debug ilpower powerman** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

Command Default このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースの **debug ilpower powerman** コマンドの出力例を示します。

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
  is done by proto CDP
Port Gil/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gil/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level[] = 2640 0 0 0 0
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) setting ICUT_OFF threshold
to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gil/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGil/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gil/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gil/0/48) setting ICUT_OFF threshold
to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notifylldp_power_via_mdi_tlvGil/0/48 pwralloc0
```

```
Mar 8 16:35:18.116: Gi1/0/48 AUTO PORT PWR Alloc130 Request 130
Mar 8 16:35:18.116: Gi1/0/48: LLDP NOTIFY TLV:
(curr/prev) PSE Allocation: 13000/0
(curr/prev) PD Request : 13000/0
(curr/prev) PD Class : Class 4/
(curr/prev) PD Priority : low/unknown
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE
(curr/prev) mdi_pwr_support: 7/0
(curr/prevPower Pair) : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown
```

次に、Cisco IOS XE Gibraltar 16.10.1 以降の **debug ilpower powerman** コマンドの出力例を示します。power_request_level、PSE Allocation、および PD Request に電力の単位 (mW) が追加されています。power_request_level にゼロ以外の値のみが表示されるようになりました。

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
is done by proto CDP
Port Gi1/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level(mW) = 2640
<----- mW unit added, non-zero value display
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gi1/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGi1/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gi1/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlvGi1/0/48 pwralloc0
Mar 8 16:35:18.116: Gi1/0/48 AUTO PORT PWR Alloc130 Request 130
Mar 8 16:35:18.116: Gi1/0/48: LLDP NOTIFY TLV:
(curr/prev) PSE Allocation (mW): 13000/0
```

```
<----- mW unit added
(curr/prev) PD Request (mW) : 13000/0
<----- mW unit added
(curr/prev) PD Class : Class 4/
(curr/prev) PD Priority : low/unknown
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE
(curr/prev) mdi_pwr_support: 7/0
(curr/prevPower Pair) : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown
```

delete

指定されたファイルシステムから 1 つ以上のファイルを削除するには、ブートローダモードで **delete** コマンドを使用します。

delete *filesystem:/file-url...*

Syntax Description

filesystem: ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0**: を使用します。

/file-url... 削除するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

Command History

リリース	変更内容
------	------

Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
--------------------------	-----------------

Usage Guidelines

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

各ファイルを削除する前に確認を求めるプロンプトがデバイスによって表示されます。

Examples

次の例では、2 つのファイルを削除します。

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

ファイルが削除されたことを確認するには、**dir usbflash0**: ブートローダコマンドを入力します。

dir

指定されたファイルシステムのファイルおよびディレクトリのリストを表示するには、ブートローダモードで **dir** コマンドを使用します。

dir *filesystem:/file-url*

Syntax Description

filesystem: ファイルシステムのエイリアス。システム ボードフラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。

/file-url (任意) 表示するコンテンツが格納されているパス (ディレクトリ) およびディレクトリの名前です。ディレクトリ名はスペースで区切ります。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ディレクトリ名では、大文字と小文字が区別されます。

Examples

次の例では、フラッシュメモリ内のファイルを表示する方法を示します。

```
Device: dir flash:
Directory of flash:/
  2  -rwx      561   Mar 01 2013 00:48:15  express_setup.debug
  3  -rwx  2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
  4  -rwx    1048   Mar 01 2013 00:01:39  multiple-fs
  6  drwx     512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
645 drwx     512   Mar 01 2013 00:01:11  dc_profile_dir
647 -rwx    4316   Mar 01 2013 01:14:05  config.text
648 -rwx      5    Mar 01 2013 00:01:39  private-config.text

96453632 bytes available (25732096 bytes used)
```

Table 156: *dir* のフィールドの説明

フィールド	説明
2	ファイルのインデックス番号

フィールド	説明
-rwx	ファイルのアクセス権（次のいずれか、またはすべて） <ul style="list-style-type: none">• d: ディレクトリ• r: 読み取り可能• w: 書き込み可能• x: 実行可能
1644045	ファイルのサイズ
<date>	最終変更日
env_vars	ファイル名

exit

以前のモードに戻るか、CLI EXEC モードを終了するには、**exit** コマンドを使用します。

exit

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトの動作や値はありません。

Command Modes 特権 EXEC
グローバル コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、コンフィギュレーション モードを終了する例を示します。

```
Device(config)# exit  
Device#
```

factory-reset

お客様固有のすべてのデータを消去し、デバイスを工場出荷時の設定に戻すには、特権 EXEC モードで **factory-reset** コマンドを使用します。



Note NIST SP 800-88 Rev. 1 で説明されているように、消去は **clear** メソッドと一致します。

Standalone Device

```
factory-reset { all [secure 3-pass] | boot-vars | config }
```

Stacked Device

```
factory-reset { all [secure 3-pass] | boot-vars | config | switch switch_number | all { all [secure 3-pass] | boot-vars | config } }
```

Syntax Description		
all	NVRAM のすべての内容、現在のブートイメージ、ブート変数、起動コンフィギュレーションと実行コンフィギュレーションのデータ、およびユーザデータを含むすべての Cisco IOS イメージを消去します。	
secure 3-pass	3-pass 上書きでデバイスからすべての内容を消去します。 <ul style="list-style-type: none"> • Pass 1: すべてのアドレス可能な場所を 2 進数のゼロで上書きします。 • Pass 2: すべてのアドレス可能な場所を 2 進数の 1 で上書きします。 • Pass 3: すべてのアドレス可能な場所をランダムビットパターンで上書きします。 	
boot-vars	ユーザによって追加されたブート変数のみを消去します。	
config	スタートアップ コンフィギュレーションのみを消去します。	
switch { <i>switch_number</i> all }	選択したスイッチのコンテンツを消去します。 <ul style="list-style-type: none"> • <i>switch-number</i>: スイッチ番号を指定します。指定できる範囲は 1 ~ 16 です。 • all: スタック内のすべてのスイッチを選択します。 	
Command Default	なし	
Command Modes	特権 EXEC (#)	
Command History	リリース Cisco IOS XE Fuji 16.9.2	変更内容 このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	secure 3-pass キーワードと switch キーワード。

Usage Guidelines

factory-reset コマンドは、次のシナリオで使用されます。

- 返品許可（RMA）のためにデバイスをシスコに返送する必要がある場合は、このコマンドを使用してお客様固有のデータをすべて削除してからデバイスの RMA 証明書を取得します。
- デバイ스에保存されている重要な情報やクレデンシャルに不正にアクセスされた場合は、このコマンドを使用してデバイスを初期設定にリセットしてから再設定します。

工場出荷時の状態へのリセットプロセスが正常に完了すると、デバイスがリブートしてROMMONモードになります。

Examples

次に、**factory-reset all** コマンドを使用してデバイスのすべての内容を消去する例を示します。

```
Device> enable
Device# factory-reset all

The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
```

次に、スタック構成デバイスで初期設定へのリセットを実行する例を示します。

```
Device> enable
Device# factory-reset switch all all

The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
Chassis 1 reloading, reason - Factory Reset

Protection key not found
```

```
9300L#Oct 25 09:53:05.740: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload
fp action requested
Oct 25 09:53:07.277: %PMAN-5-EXITACTION:vp: Process manager is exiting: rp processes exit
with reload switch code
```

```
Enabling factory reset for this reload cycle
Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...
```

```
% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...
% FACTORYRESET - finish erase
```

```
% FACTORYRESET - Making File System sd1 [0]
Discarding device blocks: done
Creating filesystem with 409600 4k blocks and 102544 inodes
Filesystem UUID: fcf01664-7c6f-41ce-99f0-6dfd941701e
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912
```

```
Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

```
% FACTORYRESET - Mounting Back sd1 [0]
% FACTORYRESET - Handling Mounted sd1
% FACTORYRESET - Factory Reset Done for sd1
```

```
% FACTORYRESET - Unmounting sd3
% FACTORYRESET - Cleaning Up sd3 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...
```

```
Chassis 2 reloading, reason - Factory Reset
Dec 12 01:02:12.500: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
```

```
De
Enabling factory reset for this reload cycle
Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...
% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...
```

After this the switch will come to boot prompt. Then the customer has to boot the device from TFTP.

flash_init

flash: ファイルシステムを再初期化するには、ブートローダモードで **flash_init** コマンドを使用します。

flash_init

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default flash: ファイルシステムは、通常のシステム動作中に自動的に初期化されます。

Command Modes ブートローダ

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines flash: ファイルシステムは、通常のブート プロセス中に自動的に初期化されます。

このコマンドは、flash: ファイルシステムを手動で初期化します。たとえば、パスワードを忘れた場合には、回復手順中にこのコマンドを使用します。

help

利用可能なコマンドを表示するには、ブートローダモードで **help** コマンドを使用します。

help

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトの動作や値はありません。

Command Modes ブートローダ

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、利用可能なブートローダコマンドのリストを表示する例を示します。

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

hostname

ネットワークサーバーのホスト名を指定または変更するには、グローバル コンフィギュレーション モードで **hostname** コマンドを使用します。

hostname *name*

Syntax Description

<i>name</i>	ネットワークサーバーの新しいホスト名を指定します。
-------------	---------------------------

Command Default

デフォルトのホスト名は、「switch」です。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ホスト名は、プロンプトとデフォルトのコンフィギュレーション ファイル名で使用されます。

大文字小文字は区別されないものと思ってください。多くのインターネットソフトウェアアプリケーションでは、大文字と小文字は区別されません。名前は英語と同様に大文字で始めるのが適切であるように思われますが、規則によりコンピュータ名はすべて小文字で表示されます。詳細については、RFC 1178 の『*Choosing a Name for Your Computer*』を参照してください。

名前は ARPANET ホスト名のルールにも従う必要があります。このルールではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。名前は63文字以下にする必要があります。数字のみのホスト名を作成することは推奨されませんが、エラーが返された後にそのホスト名は受け入れられます。

```
Device(config)#hostname 123
% Hostname contains one or more illegal characters.
123(config)#
```

ホスト名は 10 文字未満にすることを推奨します。詳細については、RFC 1035 の『*Domain Names--Implementation and Specification*』を参照してください。

ほとんどのシステムでは、ホスト名と CLI のプロンプトに 30 文字のフィールドが使用されています。ホスト名の長さによっては、コンフィギュレーション モードの長いプロンプトが切り捨てられる可能性があるので注意してください。たとえば、サービス プロファイル コンフィギュレーション モードのフルプロンプトは、次のとおりです。

```
(config-service-profile)#
```

ただし、「Switch」をホスト名として使用すると、次のプロンプトだけが表示されます（ほとんどのシステムで）。

```
Switch(config-service-profil)#
```

ホスト名をさらに長くすると、表示されるプロンプトはさらに短くなります。

```
Basement-rtr2(config-service)#
```

システムに名前を割り当てる際は、この点に注意してください（**hostname** グローバル コンフィギュレーション コマンドを使用する場合）。ユーザーが CLI のナビゲーション支援としてモードプロンプトを使用すると予想される場合は、9文字以下のホスト名を割り当てる必要があります。

hostname のような文字設定に「\」（バックスラッシュ）などの特殊文字および3桁以上の数字を使用すると、誤って変換されます。

```
Device(config)#  
Device(config)#hostname \99  
% Hostname contains one or more illegal characters.
```

Examples

次の例では、ホスト名を「host1」に変更します。

```
Device(config)# hostname host1  
host1(config)#
```

install

ソフトウェア メンテナンス アップグレード (SMU) パッケージをインストールするには、特権 EXEC モードで **install** コマンドを使用します。

```
install {abort | activate | file {bootflash: | flash: | harddisk: | webui:} [auto-abort-timer timer timer
prompt-level {all | none}]} | add file {bootflash: | flash: | ftp: | harddisk: | http: | https: | rcp: | scp:
| tftp: | webui:} [activate [auto-abort-timer timer prompt-level {all | none} commit]] | commit |
auto-abort-timer stop | deactivate file {bootflash: | flash: | harddisk: | webui:} | label id {description
description | label-name name} | remove {file {bootflash: | flash: | harddisk: | webui:} | inactive }
| rollback to {base | committed | id {install-ID} | label {label-name}}}
```

Syntax Description	
abort	現在のインストール操作を終了します。
activate	<p>install add コマンドを通じて SMU が追加されているかどうかを検証します。</p> <p>このキーワードは、互換性チェックを実行し、パッケージステータスを更新します。パッケージを再起動できる場合はポストインストールスクリプトをトリガーして必要なプロセスを再起動するか、または再起動できないパッケージの場合はリロードをトリガーします。</p>
file	アクティブにするパッケージを指定します。
{ bootflash: flash: harddisk: webui: }	インストールしたパッケージのロケーションを指定します。
auto-abort-timer <i>timer</i>	(任意) 自動アボートタイマーをインストールします。
prompt-level { all none }	<p>(任意) インストールアクティビティについてのプロンプトをユーザに表示します。</p> <p>たとえば、activate キーワードはリロードが必要なパッケージに対してリロードを自動的にトリガーします。パッケージをアクティブにする前に、続行するかどうかについてユーザに確認するプロンプトが表示されます。</p> <p>all キーワードを使用するとプロンプトをイネーブルにすることができます。none キーワードはプロンプトをディセーブルにします。</p>

add	<p>ファイルをリモートロケーション（FTPまたはTFTP）からデバイスにコピーし、プラットフォームとイメージのバージョンのSMU互換性チェックを実行します。</p> <p>このキーワードは、指定したパッケージがプラットフォームで必ずサポートされるように基本の互換性チェックを実行します。</p>
{ bootflash: flash: ftp: harddisk: http: https: rcp: scp: tftp: webui: }	追加するパッケージを指定します。
commit	<p>リロード後もSMUの変更が持続されるようにします。</p> <p>パッケージをアクティブにした後、システムがアップ状態にある間、または最初のリロード後にコミットを実行できます。パッケージがアクティブになっていてもコミットされていない場合は、最初のリロード後はアクティブの状態を保ちますが、2回目のリロード後はアクティブ状態を保ちません。</p>
auto-abort-timer stop	自動アボートタイマーを停止します。
deactivate	<p>インストールしたパッケージを非アクティブにします。</p> <p>Note パッケージを非アクティブにすると、パッケージステータスも更新され、プロセスが再起動またはリロードされることがあります。</p>
label id	ラベルを付けるインストールポイントのIDを指定します。
description	指定したインストールポイントに説明を追加します。
label-name name	指定されたインストールポイントにラベル名を追加します。
remove	<p>インストールしたパッケージを削除します。</p> <p>remove キーワードは、現在非アクティブ状態のパッケージでのみ使用できます。</p>
inactive	非アクティブ状態のすべてのパッケージをデバイスから削除します。

rollback	データ モデル インターフェイス (DMI) パッケージ SMU をベースバージョン、最後にコミットされたバージョン、または既知のコミット ID にロールバックします。
to base	ベース イメージに戻します。
committed	最後のコミット操作が実行されたときのインストール状態に戻します。
id <i>install-ID</i>	特定のインストールポイント ID に戻します。有効な値は、1 ~ 4294967295 です。

Command Default

パッケージはインストールされません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.4	このコマンドがシリーズの C9200L モデルに追加されました。
Cisco IOS XE Gibraltar 16.12.1	このコマンドがシリーズの C9200 モデルに追加されました。

Usage Guidelines

SMU は、システムにインストールしてパッチ修正やセキュリティ解決をリリースされたイメージに提供ができるパッケージです。このパッケージには、パッケージの内容を記述するいくつかのメタデータとともに、リリースにパッチを適用するための最小限の一連のファイルが含まれています。

SMU をアクティブ化する前にパッケージを追加する必要があります。

パッケージは、フラッシュから削除する前に非アクティブにする必要があります。削除したパッケージは、もう一度追加する必要があります。

単一のコマンド (1 ステップのプロセス) または個別のコマンド (3 ステップのプロセス) を使用して SMU パッケージのインストール、アクティブ化、コミットを行うことができます。SMU パッケージ ファイルを 1 つのみインストールする必要がある場合は 1 ステップ プロセスを使用し、複数の SMU をインストールする必要がある場合は 3 ステップ プロセスを使用します。3 ステップ プロセスにより、インストールする SMU パッケージ ファイルが複数ある場合に必要なりロード回数が最小限に抑えられます。次の例は、両方の方法を示しています。

例: SMU のインストール (3 ステップ プロセス、flash: を使用)

次に、3 ステップ プロセスを使用して SMU パッケージをインストールする例を示します。ここでは、SMU パッケージ ファイルがデバイスのフラッシュに保存されます。

1. フラッシュから SMU パッケージ ファイルをコピーしてインストールします。

```

Device# install add file flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
install_add: START Wed Jun 10 14:17:45 IST 2020
install_add: Adding SMU

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin to the
selected switch(es)
Finished initial file syncing

*Jun 10 14:17:48.128 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install add flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.binExecuting pre
scripts....
Executing pre sripts done.
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add /flash/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin Wed Jun 10
14:18:00 IST 2020

```

show install summary コマンドを使用して、SMU パッケージファイルの追加とインストールを確認します。SMU パッケージファイルはまだアクティブ化およびコミットされていないため、ステータスは **I** です。

```

Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
SMU   I    flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C    16.9.4.0.3431
-----

Auto abort timer: inactive
-----

```

2. SMU パッケージファイルをアクティブ化します。

```

Device# install activate file flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

install_activate: START Wed Jun 10 14:19:59 IST 2020
install_activate: Activating SMU

*Jun 10 14:20:01.513 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install activate flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

This operation requires a reload of the system. Do you want to proceed? [y/n]
Executing pre scripts....
Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
  [1] SMU_ACTIVATE package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1

```

```

Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

install_activate: Reloading the box to complete activation of the SMU...
install_activate will reload the system now!

*Jun 10 14:20:22.258 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
    Chassis 1 reloading, reason - Reload command
Jun 10 14:20:28.291: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload
fp action requested
Jun 10 14:20:30.718: %PMAN-5-EXITACTION: R0/0: pvp: Proce
Jun 10 14:20:34.834: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:
Jun 10 14:20:36.053: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
    install activate SMU flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
watchdog watchdog0: watchdog did not stop!
reboot: Restarting system

```

```

Initializing Hardware...
<output truncated>

```

```

#####
Jun 10 08:52:01.806: %BOOT-5-BOOTTIME_SMU_TEMP_ACTIVE_DETECTED: R0/0: install_engine:
SMU file /flash/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin active temporary...
SMU commit is pending

Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 17:30 by mcpre

```

```
<output truncated>
```

show install summary コマンドを使用して SMU パッケージファイルのアクティブ化を確認します。SMU パッケージファイルはまだコミットされていないため、ステータスは U です。

```

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted

```

```

-----
Type  St  Filename/Version
-----
SMU   U   flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C   16.9.4.0.3431
-----

```

```

-----
Auto abort timer: active on install_activate, time before rollback - 01:41:52
-----

```

3. SMU パッケージファイルをコミットします。

```

Device# install commit
install_commit: START Wed Jun 10 14:38:42 IST 2020
install_commit: Committing SMU

*Jun 10 14:38:44.906 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
    Started install commitExecuting pre scripts....
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
    [1] SMU_COMMIT package(s) on switch 1

```

```

[1] Finished SMU_COMMIT on switch 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit /flash/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin Wed Jun
 10 14:38:58 IST 2020
*Jun 10 14:38:59.385 IST: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0:
install_engine: Completed install commit SMU

```

show install summary コマンドを使用してコミットを確認します。SMU パッケージファイルのインストール、アクティブ化、コミットが行われました。ステータスは c です。

```

Device# show install summary
[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
SMU   C   flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C   16.9.4.0.3431
-----

Auto abort timer: inactive
-----

```

show install active コマンドを使用してアクティブパッケージを確認します。

```

Device# show install active
[ Switch 1 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
SMU   C   flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C   16.9.4.0.3431
-----

```

show version コマンドを使用して、バージョンを確認します。

```

Device# show version
Cisco IOS XE Software, Version 16.09.04
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.4,
  RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 17:30 by mcpre
...

```

例: 複数の SMU のインストール (3 ステッププロセス、flash: を使用)

次に、3 ステッププロセスを使用して複数の SMU パッケージファイルをインストールする例を示します。ここでは、SMU パッケージファイルがデバイスのフラッシュに保存されます。

スイッチスタックにインストールされているSMUファイルは次のとおりです。

```
cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin および
cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
```

1. (任意) スwitchスタックの準備ができており、SMUパッケージファイルがデバイスのフラッシュ内にあることを確認します。

```
Device# show switch
Switch/Stack Mac Address : 08ec.f586.aa80 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	08ec.f586.aa80	1	V01	Ready
2	Member	7488.bb3c.f600	1	V01	Ready
3	Member	7488.bb3f.9c00	1	V01	Ready
4	Member	08ec.f5ee.1080	1	V01	Ready
5	Standby	08ec.f589.7c80	1	V01	Ready

```
Device# dir flash: | i smu
```

```
89075 -rw- 79256 Oct 26 2035 07:07:42 +00:00
cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
89082 -rw- 9656 Oct 26 2035 07:08:08 +00:00
cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
```

2. フラッシュから SMU パッケージファイルをコピーして追加します。

一度に1つの SMU パッケージファイルのみが追加されます。SMU パッケージファイルを追加する間にリロードは必要ありません。

```
Device# install add file flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
install_add: START Fri Oct 26 07:10:59 UTC 2035
Oct 26 07:11:01.695 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....
```

```
--- Starting initial file syncing ---
```

```
*Oct 26 07:11:01.643: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install add flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin[1]: Copying
flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin from switch 1 to switch 2 3 4 5
[2 3 4 5]: Finished copying to switch 2 switch 3 switch 4 switch 5
Info: Finished copying flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin to the
selected switch(es)
Finished initial file syncing
```

```
--- Starting SMU Add operation ---
```

```
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on switch 1
[1] Finished SMU_ADD on switch 1
[2] SMU_ADD package(s) on switch 2
[2] Finished SMU_ADD on switch 2
[3] SMU_ADD package(s) on switch 3
[3] Finished SMU_ADD on switch 3
[4] SMU_ADD package(s) on switch 4
[4] Finished SMU_ADD on switch 4
[5] SMU_ADD package(s) on switch 5
[5] Finished SMU_ADD on switch 5
Checking status of SMU_ADD on [1 2 3 4 5]
SMU_ADD: Passed on [1 2 3 4 5]
```

Finished SMU Add operation

```
SUCCESS: install_add Fri Oct 26 07:11:45 UTC 2035
Oct 26 07:11:46.695 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
Device#
*Oct 26 07:11:46.656: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
Completed install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
```

show install summary コマンドを使用して、最初の SMU パッケージファイルの追加を確認します。

```
Device# show install summary
[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St  Filename/Version
-----
SMU   I   flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
IMG   C   16.12.3.0.3752
-----
Auto abort timer: inactive
-----
```

2 番目の SMU パッケージファイルを追加します。

```
Device# install add file flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin

install_add: START Fri Oct 26 07:12:38 UTC 2035
Oct 26 07:12:40.782 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....

--- Starting initial file syncing ---

*Oct 26 07:12:40.743: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install add flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin[1]: Copying
flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin from switch 1 to switch 2 3 4 5
[2 3 4 5]: Finished copying to switch 2 switch 3 switch 4 switch 5
Info: Finished copying flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin to the
selected switch(es)
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on switch 1
[1] Finished SMU_ADD on switch 1
[2] SMU_ADD package(s) on switch 2
[2] Finished SMU_ADD on switch 2
[3] SMU_ADD package(s) on switch 3
[3] Finished SMU_ADD on switch 3
[4] SMU_ADD package(s) on switch 4
[4] Finished SMU_ADD on switch 4
[5] SMU_ADD package(s) on switch 5
[5] Finished SMU_ADD on switch 5
Checking status of SMU_ADD on [1 2 3 4 5]
SMU_ADD: Passed on [1 2 3 4 5]
Finished SMU Add operation

SUCCESS: install_add Fri Oct 26 07:13:24 UTC 2035
```

```
Oct 26 07:13:25.656 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
Device#
*Oct 26 07:13:25.616: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
Completed install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
```

show install summary コマンドを使用して、両方の SMU パッケージファイルの追加とインストールを確認します。両方のパッケージファイルがまだアクティブ化およびコミットされていないため、ステータスは I です。

```
Device# show install summary
```

```
[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St   Filename/Version
-----
SMU   I    flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
SMU   I    flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
IMG   C    16.12.3.0.3752
-----
```

```
-----
Auto abort timer: inactive
-----
```

3. SMU パッケージファイルをアクティブ化します。

複数の SMU を入力する場合は、（前後にスペースを入れずに）カンマを使用してファイル名を区切ります。また、合計文字数が 128 を超えないようにしてください。この手順にはリロードが含まれます。

```
Device# install activate file
flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin,cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
```

```
install_activate: START Sun Oct 28 13:23:42 UTC 2035
Oct 28 13:23:44.620 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin,cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
install_activate: Activating SMU
```

```
*Oct 28 13:23:44.581: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install activate
flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin,cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
```

```
This operation may require a reload of the system. Do you want to proceed? [y/n]y
Executing pre scripts....
```

```
Executing pre sripts done.
```

```
--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
```

```
*Oct 28 13:24:41.563: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 secondsOct 28 13:24:43.259:
%INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer: Install auto abort
timer will expire in 7200 seconds
*Oct 28 13:24:43.222: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 4 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
*Oct 28 13:24:43.192: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 3 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
*Oct 28 13:24:43.134: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 2 R0/0:
```

```

rollback_timer: Install auto abort timer will expire in 7200 seconds
*Oct 28 13:24:43.825: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 5 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds [1] SMU_ACTIVATE
package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
  [2] SMU_ACTIVATE package(s) on switch 2
  [2] Finished SMU_ACTIVATE on switch 2
  [3] SMU_ACTIVATE package(s) on switch 3
  [3] Finished SMU_ACTIVATE on switch 3
  [4] SMU_ACTIVATE package(s) on switch 4
  [4] Finished SMU_ACTIVATE on switch 4
  [5] SMU_ACTIVATE package(s) on switch 5
  [5] Finished SMU_ACTIVATE on switch 5
Checking status of SMU_ACTIVATE on [1 2 3 4 5]
SMU_ACTIVATE: Passed on [1 2 3 4 5]
Finished SMU Activate operation

install_activate: Reloading the box to complete activation of the SMU...
install_activate will reload the system now!

Chassis 4 reloading, reason - Reload command
reload fp action requested
rp processes exit with reload switch code

watchdog watchdog0: watchdog did not stop!
reboot: Restarting system

Initializing Hardware...

System Bootstrap, Version 16.12.1r [FC6], RELEASE SOFTWARE (P)
Compiled Thu 02/13/2020 12:36:08 by rel

Current ROMMON image : Primary
C9200L-24T-4G platform with 2097152 Kbytes of main memory

boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf

#####
Oct 28 13:26:55.653: %BOOT-5-BOOTTIME_SMU_TEMP_ACTIVE_DETECTED: R0/0: install_engine:
SMU file /flash/cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin active temporary... SMU
commit is pending
Oct 28 13:26:55.912: %BOOT-5-BOOTTIME_SMU_TEMP_ACTIVE_DETECTED: R0/0: install_engine:
SMU file /flash/cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin active temporary... SMU
commit is pending

Waiting for 120 seconds for other switches to boot
#####
Switch number is 4
All switches in the stack have been discovered. Accelerating discovery

```

show install summary コマンドを使用して SMU パッケージファイルのアクティブ化を確認します。両方のファイルがまだコミットされていないため、ステータスはUです。

```

Device# show install summary
[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St  Filename/Version

```

```

-----
SMU   U   flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
SMU   U   flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
IMG   C   16.12.3.0.3752
-----

```

```

-----
Auto abort timer: active on install_activate, time before rollback - 01:50:16
-----

```

4. SMU パッケージファイルをコミットします。

```

Device# install commit
install_commit: START Sun Oct 28 13:34:42 UTC 2035
Oct 28 13:34:45.202 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit

*Oct 28 13:34:45.146: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install commitinstall_commit: Committing SMU
Executing pre scripts...
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members

*Oct 28 13:35:24.436: %PLATFORM-4-ELEMENT_WARNING: Switch 1 R0/0: smand: 5/RP/0: limited
space - copy files out of flash: directory. flash: value 84% (1599 MB) exceeds warning
level 70% (1337 MB).
*Oct 28 13:35:30.587: %PLATFORM-4-ELEMENT_WARNING: Switch 1 R0/0: smand: 2/RP/0: limited
space - copy files out of flash: directory. flash: value 74% (1412 MB) exceeds warning
level 70% (1337 MB). [1] SMU_COMMIT package(s) on switch 1
[1] Finished SMU_COMMIT on switch 1
[2] SMU_COMMIT package(s) on switch 2
[2] Finished SMU_COMMIT on switch 2
[3] SMU_COMMIT package(s) on switch 3
[3] Finished SMU_COMMIT on switch 3
[4] SMU_COMMIT package(s) on switch 4
[4] Finished SMU_COMMIT on switch 4
[5] SMU_COMMIT package(s) on switch 5
[5] Finished SMU_COMMIT on switch 5
Checking status of SMU_COMMIT on [1 2 3 4 5]
SMU_COMMIT: Passed on [1 2 3 4 5]
Finished SMU Commit operation

SUCCESS: install_commit /flash/cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
/flash/cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
Sun Oct 28 13:35:52 UTC 2035
Oct 28 13:35:53.789 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit SMU

JJ22-Vore_stack-24TE#
*Oct 28 13:35:53.749: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
Completed install commit SMU

```

show install summary コマンドを使用してコミットを確認します。SMU パッケージファイルのインストール、アクティブ化、コミットが行われました。ステータスは c です。

```

Device# show install summary
[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
SMU   C   flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
-----

```

```
SMU C flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
IMG C 16.12.3.0.3752
```

```
-----
Auto abort timer: inactive
-----
```

例: SMU のインストール (3ステッププロセス、TFTP: を使用)

次に、3ステッププロセスを使用してSMUパッケージをインストールする例を示します。ここでは、SMUパッケージファイルがリモート (TFTP) ロケーションに保存されます。

1. SMU パッケージファイルを追加します。

```
Device# install add file
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

Jun 22 11:32:27.035: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Jun 22 11:32:27.035 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Downloading file
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Finished downloading file
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin to
flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....

--- Starting initial file syncing ---

025335: *Jun 22 2020 11:32:26 UTC: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0:
install_engine: Started install add
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin[1]:
Copying flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin from switch 1 to switch
2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin to the
selected switch(es)
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on switch 1
[1] Finished SMU_ADD on switch 1
[2] SMU_ADD package(s) on switch 2
[2] Finished SMU_ADD on switch 2
Checking status of SMU_ADD on [1 2]
SMU_ADD: Passed on [1 2]
Finished SMU Add operation

SUCCESS: install_add Mon Jun 22 11:32:56 UTC 2020
Jun 22 11:32:57.598: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Jun 22 11:32:57.598 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

ECSG-SEC-C9200-24P#
025336: *Jun 22 2020 11:32:57 UTC: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0:
install_engine: Completed install add SMU
```

```
flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
```

show install summary コマンドを使用して追加を確認します。

```
Device# show install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type St Filename/Version
-----
SMU I flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG C 16.12.02.0.6
-----
Auto abort timer: inactive
-----
```

2. SMU パッケージファイルをアクティブ化します。



Note (前の手順で) SMU パッケージファイルを追加するために TFTP を使用し、TFTPではなくフラッシュしてアクティブにします。@@

```
Device# install activate file flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

install_activate: START Mon Jun 22 11:37:17 UTC 2020

Jun 22 11:37:37.582: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Jun 22 11:37:37.582 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
install_activate: Activating SMU

025337: *Jun 22 2020 11:37:37 UTC: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0:
install_engine: Started install activate
flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
This operation may require a reload of the system. Do you want to proceed? [y/n]n
```

次のとおり **show version** コマンドを使用して、バージョンを確認します。

```
Device# show version
Cisco IOS XE Software, Version 16.09.04
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 17:30 by mcpre
<output truncated>
```

3. SMU パッケージファイルをコミットします。

```
Device# install commit

install_commit: START Mon Jun 22 11:38:48 UTC 2020
SUCCESS: install_commit Mon Jun 22 11:38:52 UTC 2020
Device#
```

更新パッケージがコミットされてリロードが繰り返されても持続すること確認します。

```
Device# show install summary
```

```
Active Packages:  
tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin  
Inactive Packages:  
No packages  
Committed Packages:  
tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin  
Uncommitted Packages:  
No packages  
Device#
```

Related Commands

コマンド	説明
show install	インストールパッケージに関する情報を表示します。

ip http banner

HTTP または HTTP セキュア (HTTPS) サーバーバナーを有効にするには、グローバル コンフィギュレーション モードで **ip http banner** コマンドを使用します。HTTP または HTTPS サーバーバナーを無効にするには、このコマンドの **no** 形式を使用します。

ip http banner
no ip http banner

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default HTTP または HTTPS サーバーバナーが有効ではありません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines HTTP サーバーが要求を処理しているときに、セッション ID が無効または期限切れになると、サーバーはユーザーをバナーページにリダイレクトします。ユーザーはバナーページでログイン情報を使用してログインできます。サーバーはログイン情報を検証し、要求を処理します。

Examples

次に、HTTP または HTTPS サーバーバナーを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip http banner
Device(config)# end
```

Related Commands	コマンド	説明
	ip http banner-path	HTTP または HTTPS バナーページのカスタムパスを設定します。

ip http banner-path

HTTP または HTTP セキュア (HTTPS) バナーページのカスタムパスを設定するには、グローバル コンフィギュレーション モードで **ip http banner-path** コマンドを使用します。HTTP または HTTPS バナーページのカスタムパスを無効にするには、このコマンドの **no** 形式を使用します。

ip http banner-path *path-name*
no ip http banner-path *path-name*

Syntax Description

<i>path-name</i>	HTTP または HTTPS バナーのカスタムパス。
------------------	----------------------------

Command Default

HTTP または HTTPS バナーのカスタムパスが設定されていません。

Command Modes

グローバル コンフィギュレーション (config)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ip http banner-path コマンドを使用して、ユーザーをバナーパスに誘導します。

コマンドが設定されていない場合、またはカスタムバナーパスが存在しない場合、サーバーはユーザーをデフォルトのバナーページに誘導します。

Examples

次に、HTTP または HTTPS バナーページへのパスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip http banner-path welcome
Device(config)# end
```

Related Commands

コマンド	説明
ip http banner	HTTP または HTTPS サーバーバナーを有効にします。

ip ssh bulk-mode

セキュアシェル（SSH）バルクデータ転送モードをイネーブルにするには、グローバル コンフィギュレーション モードで **ip ssh bulk-mode** コマンドを使用します。このモードをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip ssh bulk-mode
no ip ssh bulk-mode

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default SSH 一括モードが有効になっていません。

Command Modes グローバル コンフィギュレーション（config）

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

Usage Guidelines SSH 一括モードを使用すると、大量のデータ転送を伴うプロセスのスループットパフォーマンスを最適化できます。一括コピーの最適化を活用するために、セキュアコピー機能が強化されました。この操作は、他のファイル転送操作と比較して、CPU やメモリなどのシステムリソースをより多く消費するため、大きなファイルを転送するための **ip ssh bulk-mode** コマンドを有効にすることをお勧めします。システムリソースが大量にロードされている場合は、このコマンドを使用しないでください。必要なファイル転送が完了したら、このコマンドをディセーブルにします。



- Note**
- 一括データ転送モードは、時間ベースまたはボリュームベースの SSH キー再生成機能をサポートしていません。
 - 一括データ転送モードは、SSH バージョン 1 ではサポートされていません。
 - **ip ssh bulk-mode** コマンドがイネーブルになっている場合、**ip ssh window-size** コマンドを設定しないでください。

Examples

次に、SSH サーバで一括データ転送モードを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh bulk-mode
Device(config)# exit
```

l2 traceroute

レイヤ2トレースルートサーバを有効にするには、グローバルコンフィギュレーションモードで **l2 traceroute** コマンドを使用します。レイヤ2トレースルートサーバを無効にするには、このコマンドの **no** 形式を使用します。

l2 traceroute
no l2 traceroute

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

グローバル コンフィギュレーション (config#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが追加されました。

Usage Guidelines

レイヤ2トレースルートはデフォルトでは有効になっており、ユーザ データグラム プロトコル (UDP) ポート 2228 でリスニングソケットが開きます。UDP ポート 2228 を閉じてレイヤ2トレースルートを無効にするには、グローバルコンフィギュレーションモードで **no l2 traceroute** コマンドを使用します。

次に、**l2 traceroute** コマンドを使用してレイヤ2トレースルートを設定する例を示します。

```
Device# configure terminal  
Device(config)# l2 traceroute
```

license air level

Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチに接続されているワイヤレスコントローラで AIR ライセンスを設定するには、グローバル コンフィギュレーション モードで **license air level** コマンドを入力します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

license air level { **air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] }

no license air level

Syntax Description

air-network-advantage	AIR Network Advantage ライセンスレベルを設定します。
addon air-dna-advantage	(任意) アドオンの AIR DNA の Advantage ライセンスレベルを設定します。 このアドオンオプションは AIR Network Advantage ライセンスで使用できる、デフォルトのライセンスです。
air-network-essentials	AIR Network Essential ライセンスレベルを設定します。
addon air-dna-essentials	(任意) アドオンの AIR DNA の Essential ライセンスレベルを設定します。 このアドオンオプションは AIR Network Essential ライセンスで使用できます。

Command Default

AIR DNA Advantage がデフォルトのライセンスです

Command Modes

グローバル コンフィギュレーション (Device(config)#)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、このリリースで導入されるポリシーを使用したスマートライセンスで、引き続き使用および適用することができます。詳細については、「使用上のガイドライン」セクションを参照してください。

Usage Guidelines

ポリシーを使用したスマートライセンスの環境では、**license air level** コマンドを使用して、製品インスタンスで使用されているライセンスレベルを変更したり、製品インスタンスでアドオンライセンスを追加設定したりすることができます。変更はリロード後に有効になります。

設定できるライセンスは次のとおりです。

- AIR Network Essential

- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

DNA ライセンスを更新しない場合は、AIR DNA Essential または AIR DNA Advantage ライセンスレベルを設定し、期限切れになった時点で Network Advantage または Network Essentials のライセンスレベルに移行することができます。

接続しているすべてのアクセスポイントにおいて、コントローラの一意的な値プロパティを利用するために、Cisco DNA Center ライセンスが必要です。

詳細については、「[Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#)」を参照してください。

例

次に、AIR DNA Essential ライセンスレベルを設定する例を示します。

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

次に、AIR DNA Advantage ライセンスレベルを設定する例を示します。

```
Device# configure terminal
Device(config)# license air level air-network-advantage addon air-dna-advantage
```

license boot level

デバイスで新しいソフトウェアライセンスを起動するには、グローバル コンフィギュレーション モードで **license boot level** コマンドを使用します。すべてのソフトウェアライセンスをデバイスから削除するには、このコマンドの **no** 形式を使用します。

license boot level { **network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] }

no license boot level

Syntax Description	network-advantage [addon dna-advantage]	Network Advantage ライセンスを設定します。 オプションで、デジタル ネットワーク アーキテクチャ (DNA) Advantage ライセンスを設定することもできます。
	network-essentials [addon dna-essentials]	Network Essential ライセンスを設定します。 オプションで、デジタル ネットワーク アーキテクチャ (DNA) Essential ライセンスを設定することもできます。
Command Default	Network Essentials	
Command Modes	グローバル コンフィギュレーション (config)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、このリリースで導入されるポリシーを使用したスマートライセンスで、引き続き使用および適用することができます。詳細については、「使用上のガイドライン」セクションを参照してください。

Usage Guidelines Cisco Catalyst 9000 シリーズ スイッチで使用可能なソフトウェア機能は、次のように、基本またはアドオンのライセンスレベルに分類されます。

基本ライセンス:

- Network Essentials
- Network Advantage: Network Essentials ライセンスで使用可能な機能と追加機能が含まれます。

アドオンライセンス:

- DNA Essentials
- DNA Advantage: Network Essentials ライセンスで使用可能な機能と追加機能が含まれます。

基本ライセンスは永続的または永久に効力を持つライセンスです。

アドオンライセンスはサブスクリプションまたは期間ライセンスであり、3年、5年、または7年の期間にわたって購入できます。基本ライセンスは、アドオンライセンスの前提条件です。詳細については、リリース ノート を参照してください。

以下のセクションでは、以前のスマートライセンス環境およびポリシーを使用したスマートライセンス環境での **license boot level** コマンドの使用について説明します。

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、ポリシーを使用したスマートライセンスはデフォルトで有効になっており、次の目的で **license boot level** コマンドを使用できます。

- 製品インスタンスで使用されている基本またはアドオンのライセンスレベルを変更します。
たとえば、Network Essentials を使用していて、次のリロードで Network Advantage を使用する場合や、DNA Advantage を使用して次のリロードで DNA Essentials を使用する場合があります。
- 製品インスタンスで使用されているアドオンのライセンスレベルを追加または削除します。
たとえば、Network Essentials のみを使用していて、次のリロードで DNA Essentials を使用する場合、または DNA Advantage を使用しており、次のリロード後にアドオンを使用しない場合があります。

評価ライセンスまたは期限切れライセンスの概念は、ポリシーを使用したスマートライセンスには存在しません。

コマンドを設定すると、設定したライセンスは次のリロード後に有効になります。ライセンスの使用状況は引き続きデバイスに記録され、この変更されたライセンス設定情報は、次のリソース使用率測定レポート（RUMレポート）を介して CSSM に送信する必要があります。レポートの要件と頻度は、適用されるポリシーによって決まります。**show license status** コマンド出力の「使用状況レポート」の項を参照してください。ポリシーを使用したスマートライセンスの詳細については、必要なリリースのソフトウェア設定ガイドで、「System Management」>「Smart Licensing Using Policy」を参照してください。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、スマートライセンスはデフォルトで有効になっており、次の目的で **license boot level** コマンドを使用できます。

- ライセンスのダウングレードとアップグレード
- 評価ライセンスと拡張ライセンスの有効化と無効化
- アップグレードライセンスのクリア

このコマンドは、特定のモジュールのライセンス インフラストラクチャで保持されているライセンス階層ではなく、設定されたライセンスレベルで起動するようにライセンス インフラストラクチャを設定します。

- スイッチをリロードすると、ライセンス インフラストラクチャでスタートアップ コンフィギュレーションの設定にライセンスがあるかどうかを確認されます。設定にライセンスがある場合、そのライセンスでスイッチが起動します。ライセンスがない場合、ライセンス インフラストラクチャでイメージ階層に従ってライセンスが確認されます。
- 強制ブート評価ライセンスが期限切れの場合、ライセンス インフラストラクチャで通常の階層に従ってライセンスが確認されます。
- 設定されたブートライセンスがすでに期限切れになっている場合、ライセンス インフラストラクチャで階層に従ってライセンスが確認されます。

次に、次回のリロード時に Network Essentials ライセンスを設定する例を示します。

```
Device# configure terminal
Device(config)# license boot level network-essentials
Device(config)# exit
Device# copy running-config startup-config
Device# reload
```

次に、次回のリロード時に DNA Essentials ライセンスを設定する例を示します。

```
Device# configure terminal
Device(config)# license boot level network-essentials add-on dna-essentials
Device(config)# exit
Device# copy running-config startup-config
Device# reload
```

license smart (グローバル コンフィギュレーション)

製品インスタンスが Cisco Smart Software Manager (CSSM) や Cisco Smart Licensing Utility (CSLU)、または Smart Software Manager オンプレミス (SSM オンプレミス) との通信に使用するトランスポートモードや URL などのライセンス関連の設定を行い、使用状況レポートの間隔を設定し、ライセンス使用状況レポート (RUM レポート) に含めるか、または除外する必要がある情報を設定するには、グローバル コンフィギュレーションモードで **license smart** コマンドを入力します。デフォルト値に戻すには、コマンドの **no** 形式を使用します。

```
license smart { custom_id ID | enable | privacy { all | hostname | version } | proxy { address
address_hostname | port port } | reservation | server-identity-check | transport { automatic | callhome
| cslu | off | smart } | url { url | cslu cslu_or_on-prem_url | default | smart smart_url | utility
secondary_url } | usage { customer-tags { tag1 | tag2 | tag3 | tag4 } tag_value | interval interval_in_days
} | utility [ customer_info { city city | country country | postalcode postalcode | state state | street
street } ] }
```

```
no license smart { custom_id | enable | privacy { all | hostname | version } | proxy { address
address_hostname | port port } | reservation | server-identity-check | transport | url { url | cslu
cslu_or_on-prem_url | default | smart smart_url | utility secondary_url } | usage { customer-tags {
tag1 | tag2 | tag3 | tag4 } tag_value | interval interval_in_days } | utility [ customer_info { city city
| country country | postalcode postalcode | state state | street street } ] }
```

Syntax Description

custom_id ID	このオプションは CLI では使用できませんがサポートされていません。
enable	このキーワードは CLI には表示されますが、設定しても効果はありません。スマートライセンスは常に有効になっています。
privacy { all hostname version }	CSSM に送信される使用状況レポートから特定の情報を除外できます。次のオプションから選択します。 <ul style="list-style-type: none"> • all: すべての通信で最小限のライセンス情報のみを送信します。 • hostname: 通信からホスト名を除外します。 • version: 通信から製品インスタンスのエージェントのバージョン情報を除外します。

proxy { address <i>address_hostname</i> port <i>port</i> }	CSLU または CSSM とライセンス使用状況を同期するためにプロキシを設定します。つまり、トランスポートモードが license smart transport smart (CSSM) または license smart transport cslu (CSLU) の場合にのみ、このオプションを使用してプロキシを設定できます。
	ただし、トランスポートモードとして license smart transport cslu も使用する SSM オンプレミス展開では、ライセンス使用状況の同期にプロキシは設定できません。
	次のオプションを設定します。
	<ul style="list-style-type: none">• address <i>address_hostname</i>: プロキシアドレスを設定します。 <i>address_hostname</i> には、プロキシの IP アドレスまたはホスト名を入力します。• port<i>port</i>: プロキシポートを設定します。 <i>port</i> には、プロキシポート番号を入力します。
reservation	ライセンス予約機能を有効または無効にします。 Note このオプションは、CLI で使用できますが、ライセンスの予約が適用されないため、ポリシーを使用したスマートライセンシングの環境では適用されません。
server-identity-check	HTTP セキュアサーバの ID チェックを有効または無効にします。

transport { automatic | callhome | cslu | off | smart } 製品インスタンスが CSSM との通信に使用する転送モードを設定します。次のオプションから選択します。

- **automatic:** 転送モード **cslu** を設定します。
- **callhome:** 転送モードとして Call Home を有効にします。
- **cslu:** 転送モードとして CSLU を有効にします。これがデフォルトの転送モードです。

CSLU と SSM オンプレミスの両方に同じキーワードが適用されますが、URL が異なります。次の行の **cslu***cslu_or_on-prem_url* を参照してください。

- **off:** 製品インスタンスからのすべての通信を無効にします。
 - **smart:** スマート転送を有効にします。
-

```
url { url | cslu cslu_url | default | smart
      smart_url | utility secondary_url }
```

設定された転送モードの URL を設定します。次のオプションから選択します。

- **url**: 転送モードとして **callhome** を設定している場合は、このオプションを設定します。CSSM URL を次のように正確に入力します。

```
https://software.cisco.com/#module/SmartLicensing
```

no license smart url url コマンドは、デフォルトの URL に戻ります。

- **cslu cslu_or_on-prem_url**: トランスポートモードを **cslu** として設定している場合は、必要に応じて CSLU または SSM オンプレミスの URL を使用してこのオプションを設定します。

- CSLU を使用している場合は、次のように URL を入力します。

```
http://<cslu_ip_or_host>:8182/cslu/v1/pi
```

<cslu_ip_or_host>には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

no license smart url cslu cslu_or_on-prem_url コマンドは

```
http://cslu-local:8182/cslu/v1/pi
```

 に戻ります。

- SSM オンプレミスを使用している場合は、次のように URL を入力します。

```
http://<ip>/cslu/v1/pi/<tenant ID>
```

<ip>には、SSM オンプレミスをインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID>はデフォルトのローカルバーチャルアカウント ID にする必要があります。

Tip SSM オンプレミスから URL 全体を取得できます。該当するリリース (17.3.x 以降) のソフトウェア コンフィギュレーション ガイドで、「System Management」>「Smart Licensing Using Policy」>「Task Library for Smart Licensing Using Policy」>「Retrieving the Transport

URL (SSM On-Prem UI)」を参照してください。

no license smart url cslu *cslu_or_on-prem_url*
コマンドは

`http://cslu-local:8182/cslu/v1/pi` に戻ります。

- **default:** 設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。

転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます

(`https://cslu-local:8182/cslu/v1/pi`)。

転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます

(`https://smartreceiver.cisco.com/licservice/license`)。

- **smart *smart_url*:** 転送タイプとして **smart** を設定している場合は、このオプションを設定します。URL を次のように正確に入力します。

`https://smartreceiver.cisco.com/licservice/license`

このオプションを設定すると、システムは **license smart url *url*** で自動的に URL の複製を作成します。重複するエントリは無視できます。これ以上の操作は必要ありません。

no license smart url *smartsmart_url* コマンドは、デフォルトの URL に戻ります。

- **utility *smart_url*:** このオプションは CLI では使用できませんがサポートされていません。

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }

使用状況レポートの設定を構成します。次のオプションを設定できます。

- **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value*: テレメトリ用のデータモデルに含める文字列を定義します。最大 4 つの文字列 (またはタグ) を定義できます。

tag_value には、定義する各タグの文字列値を入力します。

- **interval** *interval_in_days*: レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ~ 3650 です。

この値をゼロに設定すると、適用されるポリシーの指定内容に関係なく、RUM レポートは送信されません。これは、CSLU または CSSM が受信側にある可能性があるトポロジに適用されます。

ゼロより大きい値を設定し、通信タイプが **オフ** に設定されている場合、*interval_in_days* と Ongoing reporting frequency (days): のポリシー値の間で、値の小さい方が適用されます。たとえば、*interval_in_days* が 100 に設定され、ポリシーの値が Ongoing reporting frequency (days): 90 の場合、RUM レポートは 90 日ごとに送信されます。

間隔を設定せず、デフォルトが有効な場合、レポート間隔は完全にポリシー値によって決定されます。たとえば、デフォルト値が有効で、不適用ライセンスのみが使用されている場合、ポリシーでレポートが不要と記述されていると、RUM レポートは送信されません。

utility [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] このオプションは CLI には表示されますが、サポートされていません。

Command Default

Cisco IOS XE Amsterdam 17.3.1 以前: スマートライセンスがデフォルトで有効になっています。

Cisco IOS XE Amsterdam 17.3.2a 以降: ポリシーを使用したスマートライセンシングはデフォルトで有効になっています。

Command Modes

Global config (Device(config)#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	<p>ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。</p> <ul style="list-style-type: none"> • url キーワードの下に、次のオプションが導入されました。 <pre>{ cslu cslu_url smart smart_url }</pre> • transport キーワードの下に、次のオプションが導入されました。 <pre>{ cslu off }</pre> <p>さらに、デフォルトの通信タイプが callhome から cslu に変更されました。</p> <ul style="list-style-type: none"> • usage { customer-tags { tag1 tag2 tag3 tag4 } <i>tag_value</i> interval <i>interval_in_days</i> } <p>license smart global コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました: enable、conversion automatic。</p>
	Cisco IOS XE Amsterdam 17.3.3	<p>SSM オンプレミスサポートが導入されました。SSM オンプレミス展開での製品インスタンス開始型通信の場合、既存の [no]license smart url cslucaclu_or_on-prem_url コマンドは SSM オンプレミスの URL の設定もサポートします。ただし、SSM オンプレミスに必要な URL 形式は <code>http://<ip>/cslu/v1/pi/<tenant ID></code> です。</p> <p>設定する必要がある対応するトランスポートモードも、既存のコマンド (license smart transport cslu) です。</p>

Usage Guidelines

設定したレポート間隔 (**license smart usage interval interval_in_days** コマンド) によって、製品インスタンスが RUM レポートを送信する日時が決まります。スケジュールされた間隔が通信障害と一致する場合、製品インスタンスは、スケジュールされた時間が経過した後、最大4時間 RUM レポートの送信を試みます。(通信障害が続くために) それでもレポートを送信できない場合、システムは間隔を15分にリセットします。通信障害が解消されると、レポート間隔はユーザが最後に設定した値に戻ります。

通信障害の場合に表示される可能性があるシステムメッセージは、%SMART_LIC-3-COMM_FAILED です。このエラーを解決し、レポート間隔の値を復元する方法については、該当するリリース (17.3.x 以降) のソフトウェア設定ガイドで、「System Management」 > 「Smart Licensing Using Policy」 > 「Troubleshooting Smart Licensing Using Policy」を参照してください。

- [データプライバシーの例, on page 1755](#)
- [転送タイプと URL の例, on page 1755](#)
- [使用状況レポートのオプションの例, on page 1756](#)

データプライバシーの例

次に、グローバル コンフィギュレーション モードで **license smart privacy** コマンドを使用してデータプライバシー関連情報を設定する例を示します。 **show license status** 出力には、設定された情報が表示されます。

プライベート情報は送信されません。

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

製品インスタンスのエージェントのバージョンは送信されません。

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

転送タイプと URL の例

次に、グローバル コンフィギュレーション モードで **license smart transport** および **license smart url** コマンドを使用して、転送タイプの一部を設定する例を示します。 **show license all** 出力には、設定された情報が表示されます。

トランスポート: **cslu**:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
```

```

Type: cslu
Cslu address: http://192.168.0.1:8182/cslu/v1/pi
Proxy:
  Not Configured
<output truncated>

```

トランスポート: **smart**:

```

Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>

```

使用状況レポートのオプションの例

次に、グローバル コンフィギュレーション モードで **license smart usage** コマンドを使用して、使用状況レポートの一部を設定する例を示します。**show running-config** 出力には、設定された情報が表示されます。

customer-tag オプションの設定:

```

Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01

```

現在適用されているポリシーよりも絞り込んだレポート間隔の設定:

```

Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

```

```

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

```

```

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST

```

```
Last report file write: <none>  
<output truncated>
```

license smart (特権 EXEC)

承認コードの要求または返却、リソース使用状況測定レポート (RUM レポート) の保存、製品インスタンスへのファイルのインポート、Cisco Smart Software Manager (CSSM) との信頼の確立、CSSM または Cisco Smart License Utility (CSLU)、あるいは Smart Software Manager オンプレミス (SSM オンプレミス) との製品インスタンスの同期、製品インスタンスからのライセンス情報の削除などのライセンス機能を設定するには、対応するキーワードまたは引数を指定して特権 EXEC モードで **license smart** コマンドを入力します。

```
license smart { authorization { request { add | replace } feature_name { all | local } | return { all | local } { offline [ path ] | online } } | clear eventlog | export return { all | local } feature_name | factory reset | import file_path | save { trust-request filepath_filename | usage { all | days days | rum-id rum-ID | unreported } { file file_path } } | sync { all | local } | trust idtoken id_token_value { local | all } [ force ] }
```

Syntax Description

smart	スマートライセンスのオプションを提供します。
authorization	承認コードを要求する、または承認コードを返すオプションを提供します。 認証コードは、輸出規制または輸出規制の適用タイプのライセンスを使用する場合にのみ必要です。
request	承認コードを CSSM、CSLU (CSLU は CSSM から承認コードを取得)、または SSM オンプレミスから要求し、そのコードを製品インスタンスにインストールします。
add	要求されたライセンスを既存の承認コードに追加します。新しい承認コードには、既存の承認コードのすべてのライセンスと要求されたライセンスが含まれます。
replace	既存の承認コードを置き換えます。新しい承認コードには、要求されたライセンスのみが含まれます。現在の承認コードのすべてのライセンスが返されます。 このオプションを入力すると、製品インスタンスは、削除される承認コードに対応するライセンスが使用中であるかどうかを確認します。ライセンスが使用されている場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。
<i>feature_name</i>	承認コードを要求するライセンスの名前。
all	高可用性セットアップですべての製品インスタンスに対してアクションを実行します。
local	アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。
return	CSSM のライセンスプールに承認コードを返します。

offline <i>file_path</i>	<p>製品インスタンスがCSSMに接続されていないことを意味します。承認コードはオフラインで返されます。このオプションでは、戻りコードをファイルに出力する必要があります。</p> <p>ファイルを保存するパスを指定することもできます。ファイル形式は、.txtなどの読み取り可能な任意の形式にすることができます。</p> <p>オフラインオプションを選択する場合は、CLIや保存したファイルから戻りコードをコピーしてCSSMに入力する、という追加の手順を実行する必要があります。</p>
online	製品インスタンスが接続モードであることを意味します。承認コードは、CSLUやCSSMに直接返されます。
clear eventlog	製品インスタンスからすべてのイベントログファイルをクリアします。
export return	輸出規制ライセンスの承認キーを返します。
factory reset	製品インスタンスから保存されているすべてのライセンス情報をクリアします。
import <i>filepath_filename</i>	<p>製品インスタンスにファイルをインポートします。ファイルは、承認コード、信頼コード、またはポリシーのファイルである場合があります。</p> <p><i>filepath_filename</i> には、場所（ファイル名を含む）を指定します。</p>
save	RUM レポートや信頼コード要求を保存するオプションを提供します。
trust-request <i>filepath_filename</i>	<p>アクティブな製品インスタンスの信頼コード要求を指定した場所に保存します。</p> <p><i>filepath_filename</i> には、ファイルの絶対パス（ファイル名を含む）を指定します。</p>
usage { all days <i>days</i> rum-id <i>rum-ID</i> unreported } { file <i>file_path</i> }	<p>RUM レポート（ライセンス使用状況情報）を指定した場所に保存します。次のいずれかのオプションを指定する必要があります。</p> <ul style="list-style-type: none"> • all: すべての RUM レポートを保存します。 • days <i>days</i>: 過去 <i>n</i> 日間（現在の日を除く）の RUM レポートを保存します。番号を入力します。有効範囲は 0 ~ 4294967295 です。 たとえば、3 と入力すると、過去 3 日間の RUM レポートが保存されます。 • rum-Id <i>rum-ID</i>: 指定した RUM ID を保存します。値の有効な範囲は 0 ~ 18446744073709551615 です。 • unreported: すべての未報告の RUM レポートを保存します。 <p>file <i>filepath_filename</i>: 指定した使用状況情報をファイルに保存します。ファイルの絶対パス（ファイル名を含む）を指定します。</p>

sync { all | local } CSSMまたはCSLU、あるいはSSMオンプレミスと同期して、保留中のデータを送受信します。これには、保留中のRUMレポートのアップロード、ACK応答のダウンロード、および製品インスタンスの保留中の承認コード、信頼コード、ポリシーが含まれます。

次のいずれかのオプションを入力して、製品インスタンスを指定します。

- **all:** 高可用性セットアップですべての製品インスタンスに対して同期を実行します。このオプションを選択すると、製品インスタンスは同期要求内にあるすべてのUDIのリストも送信します。
- **local:** 要求を送信するアクティブな製品インスタンス、つまり自身のUDIに対してのみ同期を実行します。これがデフォルトのオプションです。

trust idtoken
id_token_value CSSMとの信頼できる接続を確立します。
このオプションを使用するには、最初にCSSMポータルでトークンを生成する必要があります。*id_token_value*に生成されたトークン値を指定します。

force 信頼コードが製品インスタンスにすでに存在する場合でも、信頼コード要求を送信します。
信頼コードは、製品インスタンスのUDIにノードロックされます。UDIがすでに登録されている場合、CSSMは同じUDIの新規登録を許可しません。**force** キーワードを入力すると、この動作が上書きされます。

Command Default Cisco IOS XE Amsterdam 17.3.1 以前: スマートライセンスがデフォルトで有効になっています。
Cisco IOS XE Amsterdam 17.3.2a 以降: ポリシーを使用したスマートライセンシングはデフォルトで有効になっています。

Command Modes 特権 EXEC (Device#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2a	<p>ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。</p> <ul style="list-style-type: none"> • authorization { request { add replace } <i>feature_name</i> { all local } return { all local } { offline [<i>path</i>] online } } • import <i>file_path</i> • save { trust-request <i>filepath_filename</i> usage { all days <i>days</i> rum-id <i>rum-ID</i> unreported } { file <i>file_path</i> } } • sync { all local } • trust idtoken <i>id_token_value</i> { local all } [force] <p>license smart コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました。</p> <ul style="list-style-type: none"> • register idtoken <i>token_id</i> [force] • deregister • renew id { ID auth } • debug { error debug trace all } • mfg reservation { request install install file cancel } • conversion { start stop }
Cisco IOS XE Amsterdam 17.3.3	<p>SSM オンプレミスのサポートが導入されました。リソース使用状況測定レポート (RUM レポート) の保存、製品インスタンスへのファイルのインポート、製品インスタンスの同期、認証コードの返却、SSM オンプレミス展開での製品インスタンスからのライセンス情報の削除など、ライセンス関連のタスクを実行できます。</p>

Usage Guidelines

信頼コードの上書き

license smart trust idtoken コマンドを設定する際の **force** オプションのユースケース: 1つのパーティキュラーアカウントに含まれているすべての製品インスタンスに同じトークンを使用できます。製品インスタンスが1つのアカウントから別のアカウントに移動した場合 (たとえば、別のパーティキュラーアカウントの一部である高可用性設定に追加されたため)、既存の信頼コードを上書きすることが必要になる場合があります。

ライセンス情報の削除

license smart factory reset コマンドを入力すると、承認コード、RUM レポートなど、すべてのライセンス情報 (使用中のライセンスを除く) が製品インスタンスから削除されます。そのため、このコマンドは、製品インスタンスを返却する場合 (Return Material Authorization (RMA))、または永続的にデコミットする場合にのみ使用することを推奨します。また、製品インスタンスが

らライセンス情報を削除する前に CSSM に RUM レポートを送信します。これは、CSSM に最新の使用状況情報が含まれていることを確認するためです。

認証コードとライセンス予約:

認証コードとライセンス予約に関連するオプション:

- Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチのいずれにも輸出制御ライセンスまたは適用ライセンスがないため、次のコマンドは適用されません。

- **license smart authorization request { add | replace } feature_name { all | local }**

- **license smart export return**

- 返すことも可能な SLR 承認コードの場合は、次のオプションが適用可能になっている必要があります。

license smart authorization return { all | local } { offline [path] | online }

例

- [ライセンス使用状況情報の保存例, on page 1762](#)
- [信頼コードのインストールの例, on page 1762](#)
- [SLR 承認コードを返す例, on page 1763](#)

ライセンス使用状況情報の保存例

次の例は、製品インスタンスのライセンス使用状況情報を保存する方法を示しています。このオプションを使用して、エアギャップネットワークのレポート要件を満たすことができます。この例では、ファイルはまずフラッシュメモリに保存され、次に TFTP の場所にコピーされます。

```
Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

RUM レポートをファイルに保存した後、(インターネットに接続しているワークステーションや Cisco から) CSSM にアップロードする必要があります。

信頼コードのインストールの例

次の例は、信頼コードがすでに製品インスタンスにインストールされている場合に、信頼コードをインストールする方法を示しています。これには、CSSM への接続が必要です。正常なインストール後の **show license status** 出力例を次に示します。

信頼コードをインストールする前に、トークンを生成し、CSSM から対応するファイルをダウンロードする必要があります。

結果を確認するには、**show license status** コマンド (Trust Code Installed:) を使用します。

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force
Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9500-24Y4C,SN:CAT2344L4GH
          INSTALLED on Sep 04 01:01:46 2020 EDT
  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
           INSTALLED on Sep 04 01:01:46 2020 EDT
<output truncated>
```

SLR 承認コードを返す例

次の例は、SLR 承認コードを削除して返す方法を示しています。ここでは、コードがオフラインで返されず（CSSM への接続なし）。正常に返された後の **show license all** 出力例を次に示します。

```
Device> enable
Device# license smart authorization return local online
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9500-16X,SN:FCW2233A5ZV
Return code: Cr9JHx-L1x5Rj-ftwzgl-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
Device# configure terminal
Device(config)# no license smart reservation

Device# show license all
<output truncated>
License Authorizations
=====
Overall status:
  Active: UDI: PID:C9500-16X,SN:FCW2233A5ZV
          Status: NOT INSTALLED
          Last return code: Cr9JHx-L1x5Rj-ftwzgl-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
<output truncated>
```

CLI や保存したファイルから戻りコードをコピーして CSSM に入力する、という追加の手順を実行する必要があります。

license smart deregister

Cisco Smart Software Manager (CSSM) へのデバイスの登録をキャンセルするには、特権 EXEC モードで **license smart deregister** コマンドを使用します。

license smart deregister

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは廃止され、代替コマンドは使用できません。 ポリシーを使用したスマートライセンスの導入により、このリリースでは、ライセンスを登録または登録解除する必要がなくなりました。

Usage Guidelines

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、ポリシーを使用したスマートライセンスはデフォルトで有効になっています。

登録または登録解除の概念は適用されません。製品インスタンスをデコミッションする場合、または RMA プロセスを使用してデバイスをシスコに返品して交換する場合は、特権 EXEC モードで **license smart factory reset** コマンドを使用します。これにより、承認コードや RUM レポートなど、すべてのスマートライセンス情報が製品インスタンスから削除されます。また、ライセンス情報が製品インスタンスから削除される前に CSSM に RUM レポートを送信して、CSSM で最新の使用状況情報が維持されるようにすることをお勧めします。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、スマートライセンスはデフォルトで有効になっています。このライセンスモデルでは、次の目的で **license smart deregister** コマンドを使用できます。

- デバイスをインベントリから外すとき
- デバイスを再配置のために別の場所に出荷するとき
- デバイスを交換のために返品許可（RMA）プロセスを使用してシスコに返却するとき

例

次に、CSSM へのデバイスの登録を解除する例を示します。

```

Device# license smart deregister
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-AGENT_DEREG_SUCCESS: Smart Agent for Licensing
De-registration with the Cisco Smart Software Manager or satellite was successful
*Jun 25 00:20:13.291 PDT: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is Not Allowed for udi PID:ISR4461/K9,SN:FDO2213A0GL

```

Related Commands

コマンド	説明
license smart register idtoken	CSSM にデバイスを登録します。
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license usage	ライセンス使用情報を表示します。

license smart register idtoken

Cisco Smart Software Manager (CSSM) からトークンが生成されたデバイスを登録するには、特権 EXEC モードで **license smart register idtoken** コマンドを使用します。

license smart register idtoken *token_ID* {**force**}

Syntax Description	<i>token_ID</i>	CSSM からトークンが生成されたデバイス。
	force	デバイスが登録されているかどうかに関わらずデバイスを強制的に登録します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	このコマンドは廃止され、代替コマンドは使用できません。 ポリシーを使用したスマートライセンスの導入により、このリリースでは、ライセンスを登録または登録解除する必要がなくなりました。

Usage Guidelines **ポリシーを使用したスマートライセンス:** デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、ポリシーを使用したスマートライセンスはデフォルトで有効になっています。

以前のバージョンのスマートライセンスでは、Cisco Smart Software Manager (CSSM) ポータルへの登録と接続にトークンが使用されていました。ID トークンの登録は、ポリシーを使用したスマートライセンスでは必要ありません。トークン生成機能は CSSM でも引き続き使用でき、製品インスタンスが CSSM に直接接続されている場合に信頼を確立するために使用されます。構構文の詳細については、[license smart](#)（特権 EXEC）、[on page 1758](#) の **license smart trust idtoken** *id_token_value* オプションを参照してください。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、スマートライセンスはデフォルトで有効になっており、このコマンドは引き続き適用されます。

例

次に、CSSM にデバイスを登録する例を示します。

```
Device# license smart register idtoken
$T14UytrNXBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0Ab1Rmbz0%3D%0A
```

```
Registration process is in progress. Use the 'show license status' command to check the
progress and result
Device#% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 0 seconds)
```

Related Commands

コマンド	説明
license smart deregister	CSSMへのデバイスの登録をキャンセルします。
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license usage	ライセンス使用情報を表示します。

license smart renew

Cisco Smart Software Manager (CSSM) でデバイスの ID または承認を手動で更新するには、特権 EXEC モードで **license smart renew** コマンドを使用します。

license smart renew {auth | id}

Syntax Description	auth	承認を更新します。
	id	ID を更新します。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	このコマンドは廃止されました。 ポリシーを使用したスマートライセンスの導入により、ライセンスを更新する必要がなくなり、代替コマンドを使用できなくなります。

Usage Guidelines **ポリシーを使用したスマートライセンス:** デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、ポリシーを使用したスマートライセンスはデフォルトで有効になっています。

このバージョンのライセンスモデルでは、ライセンスを更新する必要はありません。すべてのライセンスは使用中であり、ライセンスの使用状況情報（リソース使用率測定レポート）を CSSM に送信するだけで済みます。ライセンスの使用状況はタイムスタンプとともにデバイスに記録され、必要なレポートワークフローは後日完了できます。使用状況のレポートに使用する方法は、実装するトポロジによって異なります。レポートの要件と頻度は、適用されるポリシーによって決まります。詳細については、必要なリリースのソフトウェア設定ガイドで、「*System Management*」 > 「*Smart Licensing Using Policy*」を参照してください。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、スマートライセンスはデフォルトで有効になっています。この

認証期間は、スマートライセンスシステムによって 30 日ごとに更新されます。ライセンスが「承認済み」または「コンプライアンス違反」の状態にある限り、認証期間が更新されます。猶予期間は、認証期間が過ぎると開始されます。猶予期間中、またはライセンスが「期限切れ」状態になると、システムは引き続き認証期間の更新を試行します。再試行に成功すると、新しい認証期間が開始されます。

例

次に、デバイスのライセンスを更新する例を示します。

```
Device# license smart renew auth
```

Related Commands

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license usage	ライセンス使用情報を表示します。

location

エンドポイントのロケーション情報を設定するには、グローバルコンフィギュレーションモードで **location** コマンドを使用します。ロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

```
location {admin-tag string | civic-location identifier {hostid} | civic-location identifier {hostid} |
elin-location {string | identifier id} | geo-location identifier {hostid} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
no location {admin-tag string | civic-location identifier {hostid} | civic-location identifier {hostid}
| elin-location {string | identifier id} | geo-location identifier {hostid} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
```

Syntax Description

admin-tag <i>string</i>	管理タグまたはサイト情報を設定します。英数字形式のサイト情報またはロケーション情報。
civic-location	都市ロケーション情報を設定します。
identifier	都市ロケーション、緊急ロケーション、地理的な場所の名前を指定します。
host	ホストの都市ロケーションや地理空間的な場所を定義します。
<i>id</i>	都市ロケーション、緊急ロケーション、地理的な場所の名前。 Note LLDP-MED スイッチ TLV での都市ロケーションの ID は 250 バイト以下に制限されます。スイッチ設定中に使用できるバッファ スペースに関するエラーメッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。
elin-location	緊急ロケーション情報 (ELIN) を設定します。
geo-location	地理空間的なロケーション情報を設定します。
prefer	ロケーション情報のソースのプライオリティを設定します。

Command Default

デフォルトの動作や値はありません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

location civic-location identifier グローバル コンフィギュレーション コマンドを入力後、都市ロケーション コンフィギュレーション モードが開始されます。**location geo-location identifier** グローバル コンフィギュレーション コマンドを入力後、ジオロケーション コンフィギュレーション モードが開始されます。

都市ロケーション ID は 250 バイトを超えてはなりません。

ホスト ID はホストの都市ロケーションや地理空間的な場所を設定します。ID がホストではない場合、ID はインターフェイスで参照できる地理空間的なテンプレートまたは都市ロケーションだけを定義します。

host キーワードは、デバイスの場所を定義します。**identifier** と **host** キーワードを使用して設定可能な都市ロケーションオプションは同じです。都市ロケーションコンフィギュレーションモードで次の都市ロケーション オプションを指定できます。

- **additional-code:** 追加都市ロケーション コードを設定します。
- **additional-location-information:** 追加都市ロケーション情報を設定します。
- **branch-road-name:** ブランチのロード名を設定します。
- **building:** 建物の情報を設定します。
- **city:** 都市名を設定します。
- **country:** 2 文字の ISO 3166 の国コードを設定します。
- **county:** 郡名を設定します。
- **default:** コマンドをデフォルト値に設定します。
- **division:** 市の地区の名前を設定します。
- **exit:** 都市ロケーション コンフィギュレーション モードを終了します。
- **floor:** 階数を設定します。
- **landmark:** 目印となる建物の情報を設定します。
- **leading-street-dir:** 町名番地に付与される方角を設定します。
- **name:** 居住者名を設定します。
- **neighborhood:** ネイバーフッド情報を設定します。
- **no:** 指定された都市ロケーション データを拒否し、デフォルト値を設定します。
- **number:** 町名番地を設定します。
- **post-office-box:** 私書箱を設定します。
- **postal-code:** 郵便番号を設定します。
- **postal-community-name:** 郵便コミュニティ名を設定します。
- **primary-road-name:** 主要道路の名前を設定します。
- **road-section:** 道路の区間を設定します。
- **room:** 部屋の情報を設定します。
- **seat:** 座席の情報を設定します。
- **state:** 州の名前を設定します。

- **street-group:** 町名番地のグループを設定します。
- **street-name-postmodifier:** 町名番地の名前のポストモディファイアを設定します。
- **street-name-premodifier:** 町名番地の名前のプレモディファイアを設定します。
- **street-number-suffix:** 町名番地の番号のサフィックスを設定します。
- **street-suffix:** 町名番地のサフィックスを設定します。
- **sub-branch-road-name:** 支線からさらに分岐した道路名を設定します。
- **trailing-street-suffix:** 後に続く町名番地のサフィックスを設定します。
- **type-of-place:** 場所のタイプを設定します。
- **unit:** 単位を設定します。

地理的ロケーションコンフィギュレーションモードで次の地理空間的なロケーション情報を指定できます。

- **altitude:** 高さの情報を階数、メートル、またはフィート単位で設定します。
- **latitude:** 度、分、秒の緯度情報を設定します。範囲は -90 ~ 90 度です。正の値は、赤道より北側の位置を示します。
- **longitude:** 度、分、秒の経度の情報を設定します。範囲は -180 ~ 180 度です。正の値は、グリニッジ子午線の東側の位置を示します。
- **resolution:** 緯度と経度の分解能を設定します。分解能値を指定しない場合、10m のデフォルト値が緯度と経度の分解能パラメータに適用されます。緯度と経度の場合、分解能の単位はメートルで測定されます。分解能の値は小数単位でも指定できます。
- **default:** デフォルトの属性によって、地理的位置を設定します。
- **exit:** 地理的ロケーションコンフィギュレーションモードを終了します。
- **no:** 指定された地理的パラメータを拒否し、デフォルト値を設定します。

ロケーション TLV をディセーブルにするには、**no lldp med-tlv-select location information** インターフェイスコンフィギュレーションコマンドを使用します。デフォルトでは、ロケーション TLV はイネーブルに設定されています。

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name "Cisco Way"
Device(config-civic)# city "San Jose"
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county "Santa Clara"
Device(config-civic)# country US
Device(config-civic)# end
```

設定を確認するには、**show location civic-location** 特権 EXEC コマンドを入力します。

次の例では、スイッチ上で緊急ロケーション情報を設定する方法を示します。

```
Device(config)# location elin-location 14085553881 identifier 1
```

設定を確認するには、**show location elin** 特権 EXEC コマンドを入力します。

次に、スイッチに、地理空間ロケーション情報を設定する例を示します。

```
Device(config)# location geo-location identifier host  
Device(config-geo)# latitude 12.34  
Device(config-geo)# longitude 37.23  
Device(config-geo)# altitude 5 floor  
Device(config-geo)# resolution 12.34
```

設定された地理空間的な場所の詳細を表示するには、**show location geo-location identifier** コマンドを使用します。

location plm calibrating

調整クライアントのパス損失測定（CCXS60）要求を設定するには、グローバルコンフィギュレーションモードで **location plm calibrating** コマンドを使用します。

location plm calibrating {multiband | uniband}

Syntax Description	<p>multiband 関連付けられた 802.11a または 802.11b/g 無線での調整クライアントのパス損失測定要求を指定します。</p> <p>uniband 関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を指定します。</p>				
Command Default	デフォルトの動作や値はありません。				
Command Modes	グローバル コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th data-bbox="350 871 618 907">リリース</th> <th data-bbox="618 871 1497 907">変更内容</th> </tr> </thead> <tbody> <tr> <td data-bbox="350 930 618 993">Cisco IOS XE Fuji 16.9.2</td> <td data-bbox="618 930 1497 993">このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	<p>単一の無線クライアントには、（無線がデュアルバンドで、2.4 GHz と 5 GHz の両方の帯域でも動作できるとしても）uniband が役立ちます。複数の無線クライアントには、multiband が役立ちます。</p> <p>次に、関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を設定する例を示します。</p> <pre>Device# configure terminal Device(config)# location plm calibrating uniband Device(config)# end</pre>				

mgmt_init

イーサネット管理ポートを初期化するには、ブートローダモードで **mgmt_init** コマンドを使用します。

mgmt_init

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトの動作や値はありません。

Command Modes ブートローダ

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines イーサネット管理ポートのデバッグ中にのみ、**mgmt_init** コマンドを使用します。

Examples

次の例では、イーサネット管理ポートを初期化する方法を示します。

```
Device: mgmt_init
```

mkdir

指定されたファイルシステムに1つ以上のディレクトリを作成するには、ブートローダモードで **mkdir** コマンドを使用します。

mkdir *filesystem:/directory-url...*

Syntax Description

filesystem: ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

/directory-url... 作成するディレクトリの名前です。ディレクトリ名はスペースで区切ります。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ディレクトリ名では、大文字と小文字が区別されます。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ディレクトリ `Saved_Configs` を作成する方法を示します。

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

1つ以上のファイルの内容を表示するには、ブートローダモードで **more** コマンドを使用します。

more *filesystem:/file-url...*

Syntax Description

filesystem: ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。

/file-url... 表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

Examples

次に、ファイルの内容を表示する例を示します。

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

no debug all

スイッチのデバッグを無効にするには、特権 EXEC モードで **no debug all** コマンドを使用します。

no debug all

Command Default デフォルトの動作や値はありません。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE リリース 16.1	このコマンドが導入されました。

Examples

次に、スイッチでデバッグを無効にする例を示します。

```
Device: no debug all
All possible debugging has been turned off.
```

rename

ファイルの名前を変更するには、ブート コンフィギュレーション モードで **rename** コマンドを使用します。

```
rename filesystem:/source-file-url filesystem:/destination-file-url
```

Syntax Description	<i>filesystem:</i>	ファイルシステムのエイリアス。USB メモリ スティックの場合は、 usbflash0: を使用します。
	<i>/source-file-url</i>	元のパス（ディレクトリ）およびファイル名です。
	<i>/destination-file-url</i>	新しいパス（ディレクトリ）およびファイル名です。

Command Default デフォルトの動作や値はありません。

Command Modes ブートローダ

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 127 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

Examples

次の例では、ファイル *config.text* の名前を *config1.text* に変更します。

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

ファイルの名前が変更されたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

request consent-token accept-response shell-access

以前に生成されたチャレンジに対する同意トークン応答を送信するには、**request consent-token accept-response shell-access** コマンドを使用します。

request consent-token accept-response shell-access *response-string*

構文の説明

構文	説明
<i>response-string</i>	応答を表す文字列を指定します。

Command Modes 特権 EXEC モード (#)

Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

Usage Guidelines 応答文字列は、チャレンジの生成から30分以内に入力する必要があります。入力しないとチャレンジが期限切れになり、新しいチャレンジの要求が必要になります。

例

次に、**request consent-token accept-response shell-access** *response-string* コマンドの出力例を示します。

```
Device# request consent-token accept-response shell-access
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
Shell access 0).
```

request consent-token generate-challenge shell-access

システムシェルアクセスに対する同意トークンチャレンジを生成するには、**request consent-token generate-challenge shell-access** コマンドを使用します。

request consent-token generate-challenge shell-access auth-timeout *time-validity-slot*

構文の説明

構文	説明
auth-timeout <i>time-validity-slot</i>	シェルアクセスを要求するタイムスロット（分）を指定します。

Command Modes

特権 EXEC モード（#）

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

Usage Guidelines

システムシェルに対する要求したタイムスロットが期限切れになると、セッションは自動的に終了します。

システムシェルアクセスの最大承認タイムアウトは7日間です。

例

次に、**request consent-token generate-challenge shell-access auth-timeout *time-validity-slot*** コマンドの出力例を示します。

```
Device# request consent-token generate-challenge shell-access auth-timeout 900
<S>*****
Device#
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation
attempt: Shell access 0).
```

request consent-token terminate-auth

システムシェルに対する同意トークンベースの承認を終了するには、**request consent-token terminate-auth** コマンドを使用します。

request consent-token terminate-auth

Command Modes

特権 EXEC モード (#)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

Usage Guidelines

システムシェルアクセスのシナリオでは、シェルを終了しても、承認タイムアウトが発生するまで承認は終了しません。

システムシェルアクセスの目的を達成したら、**request consent-token terminate-auth** コマンドを明示的に発行することによって、システムシェルの承認を強制終了することを推奨します。

request consent-token terminate-auth コマンドを使用して現在の認証を終了した場合、ユーザがシステムシェルにアクセスする際に再度認証プロセスが必要になります。

例

次に、**request consent-token terminate-auth** コマンドの出力例を示します。

```
Device# request consent-token terminate-auth shell-access
% Consent token authorization termination success
```

```
Device#
*Mar 13 01:45:39.197: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication:
Shell access 0).
Device#
```

request platform software console attach switch

メンバスイッチでセッションを開始するには、特権 EXEC モードで **request platform software console attach switch** コマンドを使用します。



Note スタッキングスイッチ（Catalyst 3650/3850/9200/9300 スイッチ）では、このコマンドはスタンバイコンソールでセッションを開始する場合にのみ使用できます。Catalyst 9500 スイッチでは、このコマンドは Stackwise Virtual セットアップでのみサポートされます。メンバスイッチでセッションを開始することはできません。デフォルトでは、すべてのコンソールはすでにアクティブであるため、アクティブなコンソールでセッションを開始する要求はエラーになります。

request platform software console attach switch { *switch-number* | **active** | **standby** } { **0/0** | **R0** }

Syntax Description

switch-number スイッチ番号を指定します。指定できる範囲は 1 ～ 9 です。

active アクティブスイッチを指定します。

Note この引数は、Catalyst 9500 スイッチではサポートされていません。

standby スタンバイスイッチを指定します。

0/0 SPA-Inter-Processor スロットが 0 で、ベイが 0 であることを指定します。

Note このオプションをスタッキングスイッチとともに使用しないでください。それはエラーになります。

R0 ルートプロセッサ スロットが 0 であることを指定します。

Command Default

デフォルトでは、スタック内のすべてのスイッチはアクティブです。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

スタンバイスイッチでセッションを開始するには、最初に設定で有効にする必要があります。

Examples

次に、スタンバイスイッチとのセッションを行う例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# redundancy
```

```
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
Device-stby> enable
Device-stby#
```

reset

システムでハードリセットを実行するには、ブートローダモードで **reset** コマンドを実行します。ハードリセットを行うと、デバイスの電源切断後に電源を投入する手順と同様に、プロセッサ、レジスタ、およびメモリの内容が消去されます。

reset

Syntax Description	このコマンドには引数またはキーワードはありません。
---------------------------	---------------------------

Command Default	デフォルトの動作や値はありません。
------------------------	-------------------

Command Modes	ブートローダ
----------------------	--------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の例では、システムをリセットする方法を示します。

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

rmdir

指定されたファイルシステムから1つ以上の空のディレクトリを削除するには、ブートローダモードで **rmdir** コマンドを使用します。

rmdir *filesystem:/directory-url...*

Syntax Description	<p><i>filesystem:</i> ファイルシステムのエイリアス。USB メモリ スティックの場合は、usbflash0: を使用します。</p> <p><i>/directory-url...</i> 削除する空のディレクトリのパス（ディレクトリ）および名前です。ディレクトリ名はスペースで区切ります。</p>				
Command Default	デフォルトの動作や値はありません。				
Command Modes	ブートローダ				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、およびコロンは使用できません。

ディレクトリを削除する前に、まずディレクトリ内のファイルをすべて削除する必要があります。デバイスは、各ディレクトリを削除する前に、確認を求めるプロンプトを出します。

例

次の例では、ディレクトリを1つ削除する方法を示します。

```
Device: rmdir usbflash0:Test
```

ディレクトリが削除されたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

sdm prefer

スイッチで使用するSDMテンプレートを指定するには、グローバルコンフィギュレーションモードで **sdm prefer** コマンドを使用します。

sdm prefer
{advanced}

Syntax Description

advanced NetFlowなどの高度な機能をサポートします。

Command Default

デフォルトの動作や値はありません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

device スタックでは、すべてのスタックメンバが、アクティブな device に保存された同一のSDMテンプレートを必要する必要があります。

新規 device がスタックに追加されると、アクティブ device に保存されたSDMコンフィギュレーションは、個々の device に設定されているテンプレートを上書きします。

例

次に、高度なテンプレートを設定する例を示します。

```
Device(config)# sdm prefer advanced  
Device(config)# exit  
Device# reload
```

service private-config-encryption

プライベート設定ファイルの暗号化を有効にするには、**service private-config-encryption** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

service private-config-encryption
no service private-config-encryption

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトの動作や値はありません。

Command Modes グローバル コンフィギュレーション (config)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次に、プライベート設定ファイルの暗号化を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# service private-config-encryption
```

Related Commands

コマンド	説明
show parser encrypt file status	プライベート設定の暗号化ステータスを表示します。

set

環境変数を設定または表示するには、ブートローダモードで **set** コマンドを使用します。環境変数は、ブートローダまたはデバイスで稼働している他のソフトウェアを制御するために使用できません。

set *variable value*

Syntax Description

変数 値 *variable* および *value* の適切な値には、次のいずれかのキーワードを使用します。

MANUAL_BOOT: デバイスの起動を自動で行うか手動で行うかを決定します。

有効な値は 1/Yes と 0/No です。0 または No に設定されている場合、ブートローダはシステムを自動的に起動します。他の値に設定されている場合は、ブートローダモードから手動でデバイスを起動する必要があります。

BOOT filesystem:/file-url: 自動起動時にロードおよび実行される実行可能ファイルのセミコロン区切りリストを識別します。

BOOT 環境変数が設定されていない場合、システムは、フラッシュファイルシステム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュファイルシステムで最初に検出した起動可能なファイルを起動しようとします。

ENABLE_BREAK: ユーザがコンソールの **Break** キーを押すと自動起動プロセスを中断できるようになります。

有効な値は 1、Yes、On、0、No、および Off です。1、Yes、または On に設定されている場合は、フラッシュファイルシステムの初期化後にコンソール上で Break キーを押すことで、自動起動プロセスを中断できます。

HELPER filesystem:/file-url: ブートローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパーファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。

PS1 prompt: ブートローダモードの場合に、コマンドラインプロンプトとして使用する文字列を指定します。

CONFIG_FILE flash:/file-url: Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。

BAUD rate: コンソールのボーレートに使用するビット数/秒 (b/s) を指定します。コンフィギュレーションファイルに別の設定が指定されていない限り、CiscoIOS ソフトウェアはブートローダからボーレート設定を継承し、この値を引き続き使用します。指定できる範囲は 0 ~ 128000 b/s です。有効値は、50、75、110、150、300、600、1200、1800、2000、2400、3600、4800、7200、9600、14400、19200、28800、38400、56000、57600、115200、および 128000 です。

最も一般的な値は、300、1200、2400、9600、19200、57600、および 115200 です。

SWITCH_NUMBER *stack-member-number*: スタックメンバのメンバ番号を変更します。

SWITCH_PRIORITY *priority-number*: スタックメンバのプライオリティ値を変更します。

Command Default

環境変数のデフォルト値は、次のとおりです。

MANUAL_BOOT: No (0)

BOOT: ヌルストリング

ENABLE_BREAK: No (Off または 0) (コンソール上で Break キーを押して自動起動プロセスを中断することはできません)。

HELPER: デフォルト値はありません (ヘルパーファイルは自動的にロードされません)。

PS1 デバイス:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1



Note 値が設定された環境変数は、各ファイルのフラッシュファイルシステムに保管されます。ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。

このファイルに表示されていない変数には値がありません。表示されていればヌルストリングであっても値があります。ヌルストリング (たとえば “”) が設定されている変数は、値が設定された変数です。

多くの環境変数は事前に定義されており、デフォルト値が設定されています。

Command Modes

ブートローダ

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

環境変数は大文字と小文字の区別があり、指定どおりに入力する必要があります。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保管されません。

通常的环境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**boot manual** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

BOOT 環境変数は、**boot system filesystem:/file-url** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ENABLE_BREAK 環境変数は、**boot enable-break** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

HELPER 環境変数は、**boot helper filesystem: /file-url** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

CONFIG_FILE 環境変数は、**boot config-file flash:/file-url** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_NUMBER 環境変数は、**switch current-stack-member-number renumber new-stack-member-number** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_PRIORITY 環境変数は、**device stack-member-number priority priority-number** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ブートローダのプロンプト文字列 (PS1) には、等号 (=) を除く、出力可能な文字列を 120 文字まで指定できます。

例

次に、SWITCH_PRIORITY 環境変数を設定する例を示します。

```
Device: set SWITCH_PRIORITY 2
```

設定を確認するには、**set** ブートローダコマンドを使用します。

show avc client

上位アプリケーションの数に関する情報を表示するには、特権 EXEC モードで **show avc client** コマンドを使用します。

show avc client *client-mac* **top n application** [**aggregate** | **upstream** | **downstream**]

Syntax Description

client *client-mac* クライアントの MAC アドレスを指定します。

top n application 特定のクライアントの上位「N」個のアプリケーションの数を指定します。

Command Default

デフォルトの動作や値はありません。

Command Modes

特権 EXEC

Command History

リリース 変更内容
ス

このコマンドが導入されました。

次に、**show avc client** コマンドの出力例を示します。

デバイス# **sh avc client 0040.96ae.65ec top 10 application aggregate**

Cumulative Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	7343	449860	61	94
2	unknown	99	13631	137	3
3	dhcp	18	8752	486	2
4	http	18	3264	181	1
5	tftp	9	534	59	0
6	dns	2	224	112	0

Last Interval(90 seconds) Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	9	540	60	100

show bootflash:

ファイルシステムに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show bootflash:** コマンドを使用します。

show bootflash: [**all** | **filesys** | **namesort** | **sizesort** | **timesort**]

Syntax Description	all	(任意) 可能なすべてのフラッシュ情報を表示します。
	filesys	(任意) フラッシュシステム情報を表示します。
	namesort	(任意) 出力をファイル名でソートします。
	sizesort	(任意) 出力をファイルサイズでソートします。
	timesort	(任意) 出力をタイムスタンプでソートします。

Command Default	ユーザ EXEC (>) 特権 EXEC (#)
-----------------	-----------------------------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.1	次のキーワードが導入されました。 <ul style="list-style-type: none"> • namesort • sizesort • timesort

例:

次に、**show bootflash: all** コマンドの出力例を示します。

```
Device# show bootflash: all
-#- --length-- -----date/time----- path
2      4096 May 11 2020 16:49:01.0000000000 +00:00 .installer
3      4096 Feb 27 2020 15:03:50.0000000000 +00:00 .installer/issu_crash
4          12 May 05 2020 22:06:48.0000000000 +00:00 .installer/issu_crash/fru_crash
5          50 May 11 2020 16:40:40.0000000000 +00:00 .installer/last_pkgconf_shasum
```

show bootflash:

```
6      6 Feb 27 2020 16:33:59.0000000000 +00:00 .installer/install_issu_pid
7      13 Feb 27 2020 21:05:35.0000000000 +00:00 .installer/install_issu_prev_state
8      17 Feb 27 2020 21:05:36.0000000000 +00:00 .installer/install_issu_state
9      13 May 11 2020 16:41:12.0000000000 +00:00 .installer/watchlist
10     8 Feb 28 2020 18:04:31.0000000000 +00:00 .installer/crdu_frus
11     0 Mar 01 2020 18:01:09.0000000000 +00:00 .installer/.install_add_pkg_list.prev.txt
12    1729 Mar 01 2020 18:02:54.0000000000 +00:00 .installer/install_add_oper.log
13     5 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_global_trans_lock
14    10 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_state
15   33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config
16     396 May 11 2020 16:41:02.0000000000 +00:00 boothelper.log
17    4096 May 11 2020 16:40:42.0000000000 +00:00 rpr
18     80 May 11 2020 16:40:42.0000000000 +00:00 rpr/RPR_log.txt
19     80 May 05 2020 22:10:45.0000000000 +00:00 rpr/RPR_log_prev.txt
20   2183 May 11 2020 16:40:42.0000000000 +00:00 bootloader_evt_handle.log
21    4096 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh
22     965 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key
23     630 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key.pub
24   1675 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key
25     382 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key.pub
26     668 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key
27     590 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key.pub
28     492 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key
29     162 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key.pub
30     387 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key
31     82 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key.pub
32    4096 Dec 24 2019 15:24:41.0000000000 +00:00 core
33    4096 May 11 2020 16:41:29.0000000000 +00:00 core/modules
34    4096 May 05 2020 22:11:47.0000000000 +00:00 .prst_sync
35    4096 Mar 01 2020 18:17:15.0000000000 +00:00 .rollback_timer
36    4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script
37    4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script/sss
```

```

38      4096 Apr 24 2020 18:56:40.0000000000 +00:00 tech_support
39      15305 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmp-snooping.tcl
40      1612 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmpsn_dump.tcl
.
.
.

```

次に、**show bootflash: sizesort** コマンドの出力例を示します。

```

Device# show bootflash: sizesort
-#- --length-- -----date/time----- path
126 968337890 Mar 27 2020 18:06:17.0000000000 +00:00 cat9k_iosxe.CSCvt37598.bin
136 967769293 May 05 2020 21:50:33.0000000000 +00:00 cat9k_iosxe.CSCvu05574
124 967321806 Mar 23 2020 18:48:45.0000000000 +00:00 cat9k_ts_2103.bin
133 951680494 Apr 13 2020 19:46:35.0000000000 +00:00
cat9k_iosxe.2020-04-13_17.34_rakoppak.SSA.bin
130 950434163 Apr 09 2020 09:03:47.0000000000 +00:00
cat9k_iosxe.2020-04-09_13.49_rakoppak.SSA.bin
132 950410332 Apr 09 2020 07:29:57.0000000000 +00:00
cat9k_iosxe.2020-04-09_12.28_rakoppak.SSA.bin
134 948402972 Apr 17 2020 23:02:04.0000000000 +00:00 cat9k_iosxe.tla.bin

77 810146146 Feb 27 2020 15:41:42.0000000000 +00:00 cat9k_iosxe.16.12.01c.SPA.bin
88 701945494 Feb 27 2020 16:23:55.0000000000 +00:00 cat9k_iosxe.16.09.03.SPA.bin
101 535442436 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-rpbase.16.12.01c.SPA.pkg
86 88884228 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-espbase.16.12.01c.SPA.pkg
104 60167172 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipspace.16.12.01c.SPA.pkg
102 43111770 Mar 01 2020 18:02:07.0000000000 +00:00 cat9k-rpboot.16.12.01c.SPA.pkg
15 33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config
131 33554432 May 11 2020 16:42:39.0000000000 +00:00 nvram_config_bkup
103 31413252 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipbase.16.12.01c.SPA.pkg
105 22676484 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-srdriver.16.12.01c.SPA.pkg
85 14226440 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-cc_srdriver.16.12.01c.SPA.pkg
.
.
.

```

show debug

スイッチで使用できるすべての `debug` コマンドを表示するには、特権 EXEC モードで `show debug` コマンドを使用します。

show debug

show debug condition *Condition identifier* / *All conditions*

Syntax Description	<i>Condition identifier</i> 使用される条件識別子の値を設定します。範囲は、1～1000です。 <i>All conditions</i> 使用可能なすべての条件付きデバッグ オプションを表示します。				
Command Default	デフォルトの動作や値はありません。				
Command Modes	特権 EXEC				
Command History	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS XE リリース 16.1</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS XE リリース 16.1	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE リリース 16.1	このコマンドが導入されました。				

Usage Guidelines デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、`debug` コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、`debug` コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間帯を選んでデバッグを実行すると、`debug` コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

Examples

次に、`show debug` コマンドの出力例を示します。

```
Device# show debug condition all
```

デバッグを無効にするには、`no debug all` コマンドを使用します。

show env xps

Cisco eXpandable Power System (XPS) 2200 のバジェット配分、設定、電力、およびシステム電源情報を表示するには、特権 EXEC モードで **show env xps** コマンドを使用します。

```
show env xps { budgeting | configuration | port [ all | number ] | power | system |
thermal | upgrade | version }
```

Syntax Description		
budgeting		XPS 電力バジェットの配分（電源スタックに含まれるすべてのスイッチに対する電力の割り当て量とバジェット量）を表示します。
configuration		power xps 特権 EXEC コマンドを実行した結果の設定を表示します。XPS 設定は XPS に保存されます。show env xps configuration コマンドを入力すると、デフォルト以外の設定が取得されます。
port [all number]		すべてのポートまたは指定の XPS ポートの設定とステータスを表示します。ポート番号は、1～9 です。
power		XPS 電源装置のステータスを表示します。
system		XPS システム ステータスを表示します。
thermal		XPS 温度ステータスを表示します。
upgrade		XPS アップグレードステータスを表示します。
version		XPS バージョンの詳細を表示します。

Command Modes 特権 EXEC

Command History

リリース	変更内容
12.2(55)SE1	このコマンドが導入されました。

Usage Guidelines XPS 2200 の情報を表示するには、**show env xps** 特権 EXEC コマンドを使用します。

Examples

次に、show env xps budgeting コマンドの出力例を示します。

```
Switch#
=====

XPS 0101.0100.0000 :
=====
Data           Current   Power    Power Port  Switch #  PS A  PS B  Role-State
Committed
```

```

Budget
----- 1 - - 715 SP-PS
  223
 1543
 2 - - - SP-PS 223 223
 3 - - - - - -
 4 - - - - - -
 5 - - - - - -
 6 - - - - - -
 7 - - - - - -
 8 - - - - - -
 9 1 1100 - RPS-NB 223 070
XPS - - 1100 - -

```

次に、show env xps configuration コマンドの出力例を示します。

```

Switch# show env xps configuration
=====
XPS 0101.0100.0000 :
=====
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4

```

次に、show env xps port all コマンドの出力例を示します。

```

Switch#
XPS 010

-----
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 1
Data stack switch # : - Configured role      : Auto-SP
Run mode           : SP-PS : Stack Power Power-Sharing Mode
Cable faults       : 0x0 XPS 0101.0100.0000 Port 2
-----
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 2
Data stack switch # : - Configured role      : Auto-SP
Run mode           : SP-PS : Stack Power Power-Sharing Mode
Cable faults       : 0x0 XPS 0101.0100.0000 Port 3
-----
Port name          : -
Connected          : No
Mode               : Enabled (On)
Priority           : 3
Data stack switch # : - Configured role      : Auto-SP Run mode           : -
Cable faults       :
<output truncated>

```

次に、show env xps power コマンドの出力例を示します。

```

=====
XPS 0101.0100.0000 :
=====

```

```

Port-Supply SW PID                               Serial#      Status      Mode Watts
-----
XPS-A                Not present
XPS-B                NG3K-PWR-1100WAC  LIT13320NTV OK           SP   1100
1-A                  - -
1-B                  - -
2-A                  - -
2-B                  - -
9-A                  100WAC           LIT141307RK OK           RPS  1100
9-B                  esent

```

次に、show env xps system コマンドの出力例を示します。

```

Switch#
=====

XPS 0101.0100.0000 :
=====
XPS                Cfg  Cfg      RPS Switch  Current  Data Port  XPS Port Name
Mode Role      Pri Conn  Role-State  Switch #
-----
1      -                On  Auto-SP  1  Yes      SP-PS      -
2      -                On  Auto-SP  2  Yes      SP-PS      -
3      -                On  Auto-SP  3  No       -          -
4      none            On  Auto-SP  5  No       -          -
5      -                Off Auto-SP  6  No       -          -
6      -                On  Auto-SP  7  No       -          -
7      -                On  Auto-SP  8  No       -          -
8      -                On  Auto-SP  9  No       -          -
9      test            On  Auto-SP  4  Yes      RPS-NB

```

次に、show env xps thermal コマンドの出力例を示します。

```

Switch#
=====

XPS 0101.0100.0000 :
=====
Fan  Status
----  -
1    OK
2    OK
3    NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK

```

次に、アップグレードが実行されていない場合の show env xps upgrade コマンドの出力例を示します。

```

Switch# show env xps upgrade
No XPS is connected and upgrading.

```

次に、アップグレードが進行中の場合の show env xps upgrade コマンドの出力例を示します。

```

Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
-----
1  Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has

```

```

started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-----
1 Receiving 1%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.

```

次に、`show env xps version` コマンドの出力例を示します。

```

Switch# show env xps version
=====
XPS 0022.bdd7.9b14:
=====
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18

```

Table 157: 関連コマンド

コマンド	説明
power xps (グローバル コンフィギュレーション コマンド)	XPS と XPS ポートの名前を設定します。
power xps (特権 EXEC コマンド)	XPS ポートとシステムを設定します。

show flow monitor

Flexible NetFlow フローモニタのステータスと統計情報を表示するには、特権 EXEC モードで **show flow monitor** コマンドを使用します。

```
show flow monitor [broker [detail | picture] | [name] monitor-name [cache [format {csv | record | table}]] | provisioning | statistics]
```

Syntax Description	
broker	(任意) フローモニタのブローカの状態に関する情報を表示します。
detail	(任意) フローモニタのブローカに関する詳細情報を表示します。
picture	(任意) ブローカ状態の画像を表示します。
name	(任意) フローモニタの名前を指定します。
<i>monitor-name</i>	(任意) 事前に設定されたフローモニタの名前。
cache	(任意) フローモニタのキャッシュの内容を表示します。
format	(任意) ディスプレイ出力のフォーマットオプションのいずれかを使用することを指定します。
csv	(任意) フローモニタのキャッシュの内容をカンマ区切り値 (CSV) 形式で表示します。
record	(任意) フローモニタのキャッシュの内容をレコード形式で表示します。
table	(任意) フローモニタのキャッシュの内容を表形式で表示します。
provisioning	(任意) フローモニタのプロビジョニング情報を表示します。
statistics	(任意) フローモニタの統計情報を表示します。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **cache** キーワードでは、デフォルトでレコード形式が使用されます。

show flowmonitor *monitor-name* **cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローの識別に Flexible NetFlow が使用するキーフィールドです。 **show flow monitor** *monitor-name* **cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、Flexible NetFlow がキャッシュの追加データとして値を収集する非キーフィールドです。

Examples

次の例では、フロー モニタのステータスを表示します。

```

デバイス# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:     flow-record-1
  Flow Exporter:   flow-exporter-1
                  flow-exporter-2

  Cache:
    Type:           normal
    Status:         allocated
    Size:           4096 entries / 311316 bytes
    Inactive Timeout: 15 secs
    Active Timeout: 1800 secs
    Update Timeout: 1800 secs

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 158: show flow monitor monitor-name フィールドの説明

フィールド	説明
Flow Monitor	設定したフロー モニタの名前。
説明	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
Flow Record	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フロー モニタに割り当てられたエクスポート。
Cache	フロー モニタのキャッシュに関する情報。
Type	フロー モニタのキャッシュ タイプ。 次の値が可能です。 <ul style="list-style-type: none"> • immediate: フローは即座に期限切れになります。 • normal: フローは通常どおり期限切れになります。 • Permanent: フローは期限切れになりません。
Status	フロー モニタのキャッシュのステータス。 次の値が可能です。 <ul style="list-style-type: none"> • allocated: キャッシュが割り当てられています。 • being deleted: キャッシュが削除されています。 • not allocated: キャッシュが割り当てられていません。
Size	現在のキャッシュ サイズ。

フィールド	説明
Inactive Timeout	非アクティブ タイムアウトの現在の値（秒単位）。
Active Timeout	アクティブ タイムアウトの現在の値（秒単位）。
Update Timeout	更新タイムアウトの現在の値（秒単位）。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表示します。

```

デバイス# show flow monitor FLOW-MONITOR-1 cache
Cache type:                Normal (Platform cache)
Cache size:                Unknown
Current entries:          1

Flows added:              3
Flows aged:               2
  - Active timeout      ( 300 secs)  2

DATALINK MAC SOURCE ADDRESS INPUT:    0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT: 6400.F125.59E6
IPV6 SOURCE ADDRESS:                2001:DB8::1
IPV6 DESTINATION ADDRESS:           2001:DB8::1
TRNS SOURCE PORT:                   1111
TRNS DESTINATION PORT:              2222
IP VERSION:                         6
IP PROTOCOL:                        6
IP TOS:                             0x05
IP TTL:                             11
tcp flags:                          0x20
counter bytes long:                 132059538
counter packets long:               1158417

```

次の表で、この出力に表示される重要なフィールドを説明します。

Table 159: show flow monitor monitor-name cache フィールドの説明

フィールド	説明
Cache type	フローモニタのキャッシュタイプ。この値は常に normal となります。これが唯一サポートされているキャッシュタイプです。
Cache Size	キャッシュ内のエントリ数。
Current entries	キャッシュ内の使用中のエントリ数。
Flows added	キャッシュの作成後にキャッシュに追加されたフロー。
Flows aged	キャッシュの作成後に期限切れになったフロー。
Active timeout	アクティブ タイムアウトの現在の値（秒単位）。
Inactive timeout	非アクティブ タイムアウトの現在の値（秒単位）。

フィールド	説明
DATALINK MAC SOURCE ADDRESS INPUT	入力パケットの MAC 送信元アドレス。
DATALINK MAC DESTINATION ADDRESS INPUT	入力パケットの MAC 宛先アドレス。
IPV6 SOURCE ADDRESS	IPv6 送信元アドレスです。
IPV6 DESTINATION ADDRESS	IPv6 宛先アドレス。
TRNS SOURCE PORT	トランスポート プロトコルの送信元ポート。
TRNS DESTINATION PORT	トランスポート プロトコルの宛先ポート。
IP VERSION	IP バージョン。
IP PROTOCOL	プロトコル番号。
IP TOS	IP タイプ オブ サービス (ToS) の値。
IP TTL	IP 存続可能時間 (TTL) の値。
tcp flags	TCP フラグの値。
counter bytes	カウントされたバイト数。
counter packets	カウントされたパケット数。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表形式で表示します。

```

デバイス# show flow monitor FLOW-MONITOR-1 cache format table
Cache type:                Normal (Platform cache)
Cache size:                Unknown
Current entries:          1

Flows added:              3
Flows aged:               2
  - Active timeout      ( 300 secs)  2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes long
pkts long
=====
0000.0000.1000          6400.F125.59E6          2001:DB8::1    2001:DB8:1::1
      1111          2222          6          6 0x05          11 0x20          132059538
1158417

```

次の例では、FLOW-MONITOR-IPv6 という名前のフロー モニタ (キャッシュに IPv6 データを格納) のステータス、統計情報、およびデータをレコード形式で表示します。

```
デバイス# show flow monitor name FLOW-MONITOR-IPv6 cache format record
Cache type:                               Normal (Platform cache)
Cache size:                               Unknown
Current entries:                          1

Flows added:                              3
Flows aged:                               2
  - Active timeout      (   300 secs)     2

DATALINK MAC SOURCE ADDRESS INPUT:        0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:    6400.F125.59E6
IPV6 SOURCE ADDRESS:                      2001::2
IPV6 DESTINATION ADDRESS:                 2002::2
TRNS SOURCE PORT:                         1111
TRNS DESTINATION PORT:                    2222
IP VERSION:                               6
IP PROTOCOL:                              6
IP TOS:                                   0x05
IP TTL:                                   11
tcp flags:                                0x20
counter bytes long:                       132059538
counter packets long:                     1158417
```

次の例では、フロー モニタのステータスと統計情報を表示します。

```
デバイス# show flow monitor FLOW-MONITOR-1 statistics
Cache type:                               Normal (Platform cache)
Cache size:                               Unknown
Current entries:                          1

Flows added:                              3
Flows aged:                               2
  - Active timeout      (   300 secs)     2
```

show install

インストールパッケージに関する情報を表示するには、特権 EXEC モードで **show install** コマンドを使用します。

show install {**active** | **committed** | **inactive** | **log** | **package** {**bootflash:** | **flash:** | **webui:**} | **rollback** | **summary** | **uncommitted**}

Syntax Description		
active		アクティブなパッケージに関する情報を表示します。
committed		永続的なパッケージのアクティベーションを表示します。
inactive		非アクティブなパッケージを表示します。
log		ログインストレーションバッファに格納されているエントリを表示します。
package		説明、再起動情報、パッケージ内のコンポーネントなど、パッケージに関するメタデータ情報を表示します。
{ bootflash: flash: harddisk: webui: }		インストールパッケージのロケーションを指定します。
rollback		保存されているインストレーションに関連付けられたソフトウェアセットを表示します。
summary		アクティブ、非アクティブ、コミット済み、廃止されたパッケージのリストに関する情報を表示します。
uncommitted		非永続的なパッケージのアクティベーションを表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.4	このコマンドがシリーズの C9200L モデルに追加されました。
	Cisco IOS XE Gibraltar 16.12.1	このコマンドがシリーズの C9200 モデルに追加されました。

Usage Guidelines インストールパッケージのステータスを表示するには、**show** コマンドを使用します。

例

次の出力例は、**show install summary** コマンドを使用して、アクティブ、非アクティブ、コミット済み、およびコミットされていないパッケージに関する情報を表示します。ここでは、SMUパッケージファイル `cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin` がアクティブでコミットされています。

```
Device# show install summary

Active Packages:
  tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Inactive Packages:
  No packages
Committed Packages:
  tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Uncommitted Packages:
  No packages
Device#
```

下の表に、ディスプレイ内に表示される重要なフィールドのリストを示します。

Table 160: show install summary フィールドの説明

フィールド	説明
Active Packages	アクティブなインストールパッケージの名前。
Inactive Packages	非アクティブなパッケージのリスト。
Committed Packages	変更がリロード以降も存続するように、ハードディスクに変更を保存またはコミットしたインストールパッケージ。
Uncommitted Packages	非永続的なインストールパッケージのアクティブバージョン。

次に、**show install active** コマンドの出力例を示します。

```
Device# show install active

Active Packages:
tftp:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
```

次に、**show install log** コマンドの出力例を示します。

```
Device# show install log

[0|install_op_boot]: START Wed Jun 10 19:31:50 Universal 2020
[0|install_op_boot]: END SUCCESS Wed Jun 10 19:31:56 Universal 2020
```

Related Commands

コマンド	説明
install	SMUパッケージをインストールします。

show location

エンドポイントのロケーション情報を表示するには、特権 EXEC モードで **show location** コマンドを使用します。

show location

```
[admin-tag | civic-location {identifier identifier-string | interface type number | static} | custom-location {identifier identifier-string | interface type number | static} | elin-location {identifier identifier-string | interface type number | static} | geo-location {identifier identifier-string | interface type number | static} | host]
```

Syntax Description

admin-tag	管理タグまたはサイト情報を表示します。
civic-location	都市ロケーション情報を指定します。
identifier <i>identifier-string</i>	シビック ロケーション、カスタム ロケーション、または地理空間的なロケーションの情報識別子。
interface type number	インターフェイスのタイプと番号 デバイスに対する番号付け構文については、疑問符 (?) のオンラインヘルプ機能を使用してください。
static	設定されたシビック、カスタム、または地理空間的ロケーション情報を表示します。
custom-location	カスタム ロケーション情報を指定します。
elin-location	緊急ロケーション情報 (ELIN) を指定します。
geo-location	地理空間的なロケーション情報を指定します。
host	シビック、カスタム、または地理空間的なホスト ロケーション情報を指定します。

Command Default

デフォルトの動作や値はありません。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次の **show location civic-location** コマンドの出力例は、指定された識別子 (*identifier 1*) のシビックロケーション情報を表示します。

```
Device# show location civic-location identifier 1
Civic location information
-----
Identifier           : 1
County              : Santa Clara
Street number       : 3550
Building            : 19
Room                : C6
Primary road name   : Example
City                : San Jose
State               : CA
Country             : US
```

Related Commands

コマンド	説明
location	エンドポイントにロケーション情報を設定します。

show logging onboard switch uptime

システム内のすべてのモジュールまたはスイッチのすべてのリセット理由の履歴を表示するには、**show logging onboard switch uptime** コマンドを使用します。

show logging onboard switch { *switch-number* | **active** | **standby** } **uptime** [[**continuous** | **detail**] [**start** *hour day month* [*year*] [**end** *hour day month year*]] | **summary**]

Syntax Description		
switch <i>switch-number</i>		スイッチを指定します。スイッチ番号を入力します。
active		アクティブ インスタンスを指定します。
standby		スタンバイ インスタンスを指定します。
continuous		(任意) 連続データを表示します。
detail		(任意) 詳細データを表示します。
start <i>hour day month year</i>		(任意) データを表示する開始時刻を指定します。
end <i>hour day month year</i>		(任意) データを表示する終了時刻を指定します。
summary		(任意) 要約データを表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが以下に実装されました。 Cisco Catalyst 9200 シリーズ スイッチ
	Cisco IOS XE Gibraltar 16.10.1	このコマンドの出力が更新され、スタック内のメンバのリロード理由が表示されるようになりました。

次に例を示します。

次に、**show logging onboard switch active uptime continuous** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime continuous
-----
UPTIME CONTINUOUS INFORMATION
-----
Time Stamp           | Reset           | Uptime
MM/DD/YYYY HH:MM:SS | Reason         | years weeks days hours minutes
-----
```

```

06/17/2018 19:42:56 Reload 0 0 0 0 5
06/17/2018 19:56:31 Reload 0 0 0 0 5
06/17/2018 20:10:46 Reload 0 0 0 0 5
06/17/2018 20:23:48 Reload 0 0 0 0 5
06/17/2018 20:37:20 Reload Command 0 0 0 0 5
06/18/2018 17:09:23 Reload Command 0 0 0 20 5
06/18/2018 17:18:39 redundancy force-switchover 0 0 0 0 5
06/18/2018 18:33:33 Reload 0 0 0 1 5
06/18/2018 19:03:05 Reload 0 0 0 0 5
06/18/2018 19:40:30 Reload 0 0 0 0 5
06/18/2018 20:37:47 Reload 0 0 0 0 5
06/18/2018 20:51:13 Reload 0 0 0 0 5
06/18/2018 21:04:08 Reload 0 0 0 0 5
06/18/2018 21:18:23 Reload 0 0 0 0 5
06/18/2018 21:31:25 Reload 0 0 0 0 5
06/18/2018 21:45:15 Reload 0 0 0 0 5
06/18/2018 21:59:02 Reload 0 0 0 0 5
06/18/2018 22:11:41 Reload 0 0 0 0 5
06/18/2018 22:24:27 Reload 0 0 0 0 5
06/18/2018 22:39:14 Reload Command 0 0 0 0 4
06/19/2018 00:01:59 Reload Command 0 0 0 1 5
06/19/2018 00:13:21 redundancy force-switchover 0 0 0 0 5
06/19/2018 01:05:42 redundancy force-switchover 0 0 0 0 5
06/20/2018 02:37:16 redundancy force-switchover 0 0 1 1 5
06/20/2018 02:50:03 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:02:13 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:14:26 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:26:44 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:38:58 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:52:43 redundancy force-switchover 0 0 0 0 5
06/20/2018 04:05:16 redundancy force-switchover 0 0 0 0 5
.
.
.

```

次に、**show logging onboard switch active uptime detail** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime detail
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```

First customer power on : 06/10/2017 09:28:22
Total uptime           : 0 years 50 weeks 4 days 13 hours 38 minutes
Total downtime         : 0 years 15 weeks 4 days 11 hours 52 minutes
Number of resets       : 75
Number of slot changes : 9
Current reset reason   : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot           : 1
Chassis type           : 0
Current uptime         : 0 years 0 weeks 0 days 0 hours 0 minutes
-----

```

```
-----
UPTIME CONTINUOUS INFORMATION
-----
```

```

Time Stamp          | Reset          | Uptime
MM/DD/YYYY HH:MM:SS | Reason        | years weeks days hours minutes
-----
06/10/2017 09:28:22 | Reload        | 0 0 0 0 0
<snip>
09/17/2018 09:07:44 | PowerOn       | 0 0 3 15 5
09/17/2018 10:16:26 | Reload Command | 0 0 0 1 5

```

show logging onboard switch uptime

```
09/17/2018 10:59:57 PowerOn 0 0 0 0 5
```

次に、**show logging onboard switch standby uptime detail** コマンドの出力例を示します。

```
Device# show logging onboard switch standby uptime detail
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```
First customer power on : 06/10/2017 11:51:26
Total uptime           : 0 years 46 weeks 0 days 11 hours 44 minutes
Total downtime        : 0 years 20 weeks 1 days 10 hours 45 minutes
Number of resets      : 79
Number of slot changes : 13
Current reset reason   : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot          : 2
Chassis type          : 0
Current uptime        : 0 years 0 weeks 0 days 0 hours 5 minutes
-----
```

```
-----
UPTIME CONTINUOUS INFORMATION
-----
```

Time Stamp MM/DD/YYYY HH:MM:SS	Reset Reason	Uptime				
		years	weeks	days	hours	minutes
06/10/2017 11:51:26	Reload	0	0	0	0	0
<snip>						
08/10/2018 09:13:58	LocalSoft	0	0	2	5	4
08/28/2018 14:21:42	Reload Slot Command	0	0	0	3	5
08/28/2018 14:34:29	System requested reload	0	0	0	0	0
09/11/2018 09:08:15	Reload	0	0	1	8	5
09/11/2018 19:15:06	redundancy force-switchover	0	0	0	9	4
09/13/2018 16:50:18	Reload Command	0	0	1	21	6
09/17/2018 10:55:09	PowerOn	0	0	0	0	5

次に、**show logging onboard switch active uptime summary** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime summary
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```
First customer power on : 04/26/2018 21:45:39
Total uptime           : 0 years 20 weeks 2 days 12 hours 22 minutes
Total downtime        : 0 years 2 weeks 2 days 8 hours 40 minutes
Number of resets      : 1900
Number of slot changes : 18
Current reset reason   : Reload Command
Current reset timestamp : 09/26/2018 20:43:15
Current slot          : 1
Chassis type          : 91
Current uptime        : 0 years 0 weeks 5 days 22 hours 5 minutes
-----
```

show license all

すべてのライセンス情報を表示するには、特権 EXEC モードで **show license all** コマンドを入力します。このコマンドは、ステータス、承認、UDI、および使用状況の情報をすべて組み合わせて表示します。

show license all

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに関する情報が表示されるようになりました。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。

Usage Guidelines

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されません（スマートライセンスが有効になっているかどうか、関連するすべてのライセンス証明書、コンプライアンスステータスなど）。

例

[ポリシーを使用したスマートライセンスの show license all, on page 1813](#)

[スマートライセンスの show license all, on page 1816](#)

ポリシーを使用したスマートライセンスの show license all

次に、Cisco Catalyst 9500 スイッチでの **show license all** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license all
```

```
Smart Licensing Status
=====
```

```
Smart Licensing is ENABLED
License Reservation is ENABLED
Export Authorization Key:
  Features Authorized:
    <none>
Utility:
  Status: DISABLED
Smart Licensing Using Policy:
  Status: ENABLED
Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
Transport:
  Type: Transport Off
Miscellaneous:
  Custom Id: <empty>
Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Nov 29 10:50:05 2020 PDT
  Reporting Interval: 30
  Next ACK push check: <none>
  Next report push: Aug 31 10:52:05 2020 PDT
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
License Usage
=====
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 2
dna-advantage (C9500-16X DNA Advantage):
  Description: C9500-16X DNA Advantage
  Count: 2
```

```
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9500-16X DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription
Reservation:
  Reservation status: SPECIFIC INSTALLED
  Total reserved count: 2
Product Information
=====
UDI: PID:C9500-16X,SN:FCW2233A5ZV
HA UDI List:
  Active:PID:C9500-16X,SN:FCW2233A5ZV
  Standby:PID:C9500-16X,SN:FCW2233A5ZY
Agent Version
=====
Smart Agent for Licensing: 5.0.5_rel/42
License Authorizations
=====
Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
    Status: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
    Last Confirmation code: 4bfbea7f
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
    Status: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
    Last Confirmation code: 9394f196
Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
        Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
        Term Count: 1
  C9500-DNA-16X-A (C9500-16X DNA Advantage):
    Description: C9500-DNA-16X-A
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
        Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
        Term Count: 1
Purchased Licenses:
  No Purchase Information Available
Derived Licenses:
  Entitlement Tag:
  regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
  Entitlement Tag:
  regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
```

スマートライセンスの show license all

次に、**show license all** コマンドの出力例を示します。

```
Device# show license all
Smart Licensing Status
=====

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: CISCO Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Initial Registration: First Attempt Pending
  Last Renewal Attempt: SUCCEEDED on Jul 19 14:49:49 2018 IST
  Next Renewal Attempt: Jan 15 14:49:48 2019 IST
  Registration Expires: Jul 19 14:43:48 2019 IST

License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST
  Last Communication Attempt: SUCCEEDED on Jul 28 07:02:56 2018 IST
  Next Communication Attempt: Aug 27 07:02:56 2018 IST
  Communication Deadline: Oct 26 06:57:50 2018 IST

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

License Usage
=====

C9200L DNA Advantage, 48-port Term license (C9200L-DNA-A-48):
  Description: C9200L DNA Advantage, 48-port Term license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9200L Network Advantage, 48-port license (C9200L-NW-A-48):
  Description: C9200L Network Advantage, 48-port license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
=====
UDI: PID:C9200L-48P-4X, SN:JPG221300KP

Agent Version
=====
Smart Agent for Licensing: 4.4.13_rel/116
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel15)1.0.3, PK:(dev18)1.0.3

Reservation Info
=====
```

License reservation: DISABLED

Related Commands

コマンド	説明
show license status	ライセンスのコンプライアンスステータスを表示します。
show license authorization	許可コード関連情報を表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。
show license tech support	デバッグ出力を表示します。

show license authorization

ライセンス（輸出規制および適用）の承認関連情報を表示するには、特権 EXEC モードで **show license authorization** コマンドを入力します。

show license authorization

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC（Device#）

Command History

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2a	このコマンドが導入されました。

Usage Guidelines

Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチには、輸出制御または強制されたライセンスはありませんが、このコマンドを使用して、移行された SLR 承認コードを表示できます。

例

ディスプレイに表示されるフィールドについては、[Table 161: show license authorization のフィールドの説明, on page 1819](#) を参照してください。

出力例については、[show license authorization の移行された SLR 認証コードの表示, on page 1822](#) を参照してください。

Table 161: show license authorization のフィールドの説明

フィールド	説明
Overall Status	設定内にあるすべての製品インスタンスのUDI情報のヘッダー、インストールされている承認のタイプ、および設定エラー（存在する場合）。 高可用性設定では、設定内にあるすべてのUDIがリストされます。
Active: ステータス:	アクティブ製品インスタンスUDIと、それに続いてこのUDIの承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
Standby: ステータス:	スタンバイ製品インスタンスUDIと、それに続いてこのUDIの承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
Member: ステータス:	メンバー製品インスタンスUDIと、それに続いてこのUDIの承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
ERROR:	高可用性設定の設定エラーまたは不一致（存在する場合）。

フィールド	説明
承認	<p>詳細なライセンス承認情報のヘッダー。すべてのライセンス、その適用タイプ、および有効期間が表示されます。承認またはモードがアクティブにインストールされているものと一致しない場合、製品インスタンスごとにエラーが表示されます。</p> <p>このセクションは、製品インスタンスが承認コードを必要とするライセンスを使用している場合にのみ表示されます。</p>
()	ライセンス名およびライセンス名の短縮形。
説明	ライセンスの説明。
Total available count:	<p>使用可能なライセンスの合計数。</p> <p>これには、高可用性設定のすべての製品インスタンスに関して、期限切れのサブスクリプション ライセンスを含む、すべての期間のライセンス（永久ライセンスおよびサブスクリプション）が含まれます。</p>
Enforcement type	<p>ライセンスの適用タイプ。これは、次のいずれかです。</p> <ul style="list-style-type: none"> • 適用 • 非適用 • 輸出規制
Term information:	

フィールド	説明												
	<p>ライセンス期間情報を提供するヘッダー。このヘッダーには、次のフィールドが含まれることがあります。</p> <ul style="list-style-type: none"> • Active: アクティブ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 • Authorization type: インストールされている承認コードのタイプとインストール日。タイプは、SLAC、UNIVERSAL、SPECIFIED、PAK、RTU です。 • Start Date: ライセンスが特定の期間または時間の場合に、有効期間の開始日を表示します。 • Start Date: ライセンスが特定の期間または時間の場合に、有効期間の終了日を表示します。 • Term Count: ライセンス数。 • Subscription ID: ライセンスが特定の期間または時間の場合に、ID を表示します。 • License type: ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。 • Standby: スタンバイ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 • Member: メンバー製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 												
Purchased Licenses	<p>ライセンス購入情報のヘッダー。</p> <table border="1" data-bbox="609 1386 1513 1789"> <tbody> <tr> <td data-bbox="609 1386 836 1449">Active:</td> <td data-bbox="836 1386 1513 1449">アクティブ製品インスタンスとその UDI。</td> </tr> <tr> <td data-bbox="609 1449 836 1512">Count:</td> <td data-bbox="836 1449 1513 1512">ライセンス数。</td> </tr> <tr> <td data-bbox="609 1512 836 1575">Description:</td> <td data-bbox="836 1512 1513 1575">ライセンスの説明。</td> </tr> <tr> <td data-bbox="609 1575 836 1669">License type:</td> <td data-bbox="836 1575 1513 1669">ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。</td> </tr> <tr> <td data-bbox="609 1669 836 1732">Standby:</td> <td data-bbox="836 1669 1513 1732">スタンバイ製品インスタンスの UDI。</td> </tr> <tr> <td data-bbox="609 1732 836 1789">Member:</td> <td data-bbox="836 1732 1513 1789">メンバー製品インスタンスの UDI。</td> </tr> </tbody> </table>	Active:	アクティブ製品インスタンスとその UDI。	Count:	ライセンス数。	Description:	ライセンスの説明。	License type:	ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。	Standby:	スタンバイ製品インスタンスの UDI。	Member:	メンバー製品インスタンスの UDI。
Active:	アクティブ製品インスタンスとその UDI。												
Count:	ライセンス数。												
Description:	ライセンスの説明。												
License type:	ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。												
Standby:	スタンバイ製品インスタンスの UDI。												
Member:	メンバー製品インスタンスの UDI。												

show license authorization の移行されたSLR認証コードの表示

次に、ポリシーを使用してスマートライセンスに移行された SLR 承認コード（最終確認コード：）を示す **show license authorization** コマンドの出力例を示します。

```
Device# show license authorization

Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
  Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
  Last Confirmation code: 184ba6d6
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
  Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
  Last Confirmation code: 961d598f

Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
  Description: C9500 Network Advantage
  Total reserved count: 2
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9500-16X,SN:FCW2233A5ZV
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1
    Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1
  C9500-DNA-16X-A (C9500-16X DNA Advantage):
  Description: C9500-DNA-16X-A
  Total reserved count: 2
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9500-16X,SN:FCW2233A5ZV
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1
    Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
  regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
  Entitlement Tag:
  regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
```

show license data translation

ライセンスデータ転換情報を表示するには、特権 EXEC モードで **show license data** コマンドを入力します。

show license data conversion

構文の説明

このコマンドには、引数またはキーワードはありません。

Command Modes

特権 EXEC (Device#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに関する情報が表示されるようになりました。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。

Usage Guidelines

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

デバイス主導の変換は、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチではサポートされていません。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されません。

show license eventlog

ポリシーを使用したスマートライセンスに関連するイベントログを表示するには、特権EXECモードで **show license eventlog** コマンドを入力します。

show license eventlog [*days*]

Syntax Description	<i>days</i> イベントログを表示する日数を入力します。0～2147483647の範囲の値を指定できます。						
Command Modes	特権 EXEC (Device#)						
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> <tr> <td>Cisco IOS XE Amsterdam 17.3.2a</td> <td> <p>ポリシーを使用したスマートライセンスの導入により、次のイベントが追加されました。</p> <ul style="list-style-type: none"> • ポリシーのインストールと削除 • 承認コードの要求、インストール、および削除。 • 信頼コードのインストールと削除。 • ライセンス使用状況に関する承認ソース情報の追加。 </td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。	Cisco IOS XE Amsterdam 17.3.2a	<p>ポリシーを使用したスマートライセンスの導入により、次のイベントが追加されました。</p> <ul style="list-style-type: none"> • ポリシーのインストールと削除 • 承認コードの要求、インストール、および削除。 • 信頼コードのインストールと削除。 • ライセンス使用状況に関する承認ソース情報の追加。
リリース	変更内容						
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。						
Cisco IOS XE Amsterdam 17.3.2a	<p>ポリシーを使用したスマートライセンスの導入により、次のイベントが追加されました。</p> <ul style="list-style-type: none"> • ポリシーのインストールと削除 • 承認コードの要求、インストール、および削除。 • 信頼コードのインストールと削除。 • ライセンス使用状況に関する承認ソース情報の追加。 						

Usage Guidelines

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されません。

例

ポリシーを使用したスマートライセンスの [show license eventlog for One Day, on page 1824](#)

ポリシーを使用したスマートライセンスの [show license eventlog for All Events, on page 1825](#)

ポリシーを使用したスマートライセンスの show license eventlog for One Day

次に、Cisco Catalyst 9500 スイッチでの **show license eventlog** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。このコマンドは、1日分のイベントを表示するように設定されています。

```
Device# show license eventlog 1
**** Event Log ****
```

```

2020-09-11 00:50:17.693 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 00:50:50.175 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-11 08:50:17.694 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 08:50:52.804 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"

```

ポリシーを使用したスマートライセンスの show license eventlog for All Events

次に、Cisco Catalyst 9500 スイッチでの **show license eventlog** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。このコマンドは、すべてのイベントを表示するように設定されています。

```
Device# show license eventlog
```

```

**** Event Log ****

2020-09-01 15:43:42.300 UTC SAEVT_INIT_START version="4.13.14_rel/41"
2020-09-01 15:43:42.301 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization
has not been completed"
2020-09-01 15:43:42.301 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHarmfRegister"
2020-09-01 15:43:45.055 UTC SAEVT_READY
2020-09-01 15:43:45.055 UTC SAEVT_ENABLED
2020-09-01 15:43:45.088 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_LICENSE_USAGE count="0" type="destroy"
entitlementTag="regid.2018-01.com.cisco.C9500-24Y4C-A,1.0_6b065611-6552-472a-8859-ab3339550166"
2020-09-01 15:43:45.098 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"

```

show license history message

製品インスタンスと CSSM または CSLU（該当する場合）の間の通信履歴を表示するには、特権 EXEC モードで **show license history message** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングに使用します。

show license history message

Syntax Description

このコマンドにはキーワードまたは引数はありません。

Command Modes

特権 EXEC (Device#)

Command History

リリース	変更内容
------	------

Cisco IOS XE Amsterdam 17.3.2a このコマンドが導入されました。

Usage Guidelines

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

show license reservation

ライセンス予約情報を表示するには、特権 EXEC モードで **show license reservation** コマンドを入力します。

show license reservation

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC (Device#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンドは CLI で引き続き使用できますが、予約の概念がポリシーを使用したスマートライセンス環境に存在しないため、適用できません。

Usage Guidelines

コマンドは CLI で引き続き使用可能であり、対応する出力が表示されますが、ポリシーを使用したスマートライセンシングの導入により、予約の概念は適用されなくなりました。代わりに、特権 EXEC モードで **show license all** コマンドを使用して、移行された SLR ライセンスを表示します (SLR 承認コードはポリシーを使用してスマートライセンスに移行されます)。

show license status

データプライバシー、ポリシー、転送、使用状況レポート、信頼コードなどのライセンス設定に関する情報を表示するには、特権 EXEC モードで **show license status** コマンドを入力します。

show license status

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。これには、Trust code installed:、Policy in use、Policy name:、ポリシーと同様のレポート要件、および使用状況レポートに関連するフィールドが含まれます。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。

Usage Guidelines **ポリシーを使用したスマートライセンス:** デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されません。

例

ディスプレイに表示されるフィールドについては、[Table 162: ポリシーを使用したスマートライセンスの show license status のフィールドの説明, on page 1829](#) を参照してください。

ポリシーを使用したスマートライセンスの [show license status, on page 1834](#)

スマートライセンスの [show license status, on page 1835](#)

Table 162: ポリシーを使用したスマートライセンスの *show license status* のフィールドの説明

フィールド	説明
ユーティリティ	製品インスタンスで設定されているユーティリティ設定のヘッダー。
ステータス:	Status
ユーティリティレポート:	最後の試行結果:
顧客情報:	次のフィールドが表示されます。 <ul style="list-style-type: none"> • ID: • Name: • Street • City: • State: • Country: • Postal Code:
ポリシーを使用したスマートライセンス	製品インスタンスのポリシー設定のヘッダー。
ステータス:	<p>ポリシーを使用したスマートライセンスが有効になっているかどうかを示します。</p> <p>ポリシーを使用したスマートライセンスは、Cisco IOS XE Amsterdam 17.3.2以降でサポートされ、サポートされているソフトウェアイメージでは常に有効になっています。</p>

フィールド	説明	
データプライバシー:	製品インスタンスで設定されているプライバシー設定のヘッダー。	
	送信ホスト名:	ホスト名が使用状況レポートで送信されるかどうかを示す <i>yes</i> または <i>no</i> の値。
	Callhome ホスト名のプライバシー:	Call Home 機能がレポートの転送モードとして設定されているかどうかを示します。設定されている場合、次のいずれかの値が表示されます。 <ul style="list-style-type: none"> • ENABLED • DISABLED
	スマートライセンスホスト名のプライバシー:	次のいずれかの値が表示されます。 <ul style="list-style-type: none"> • ENABLED • DISABLED
	バージョンプライバシー:	次のいずれかの値が表示されます。 <ul style="list-style-type: none"> • ENABLED • DISABLED
トランスポート:	製品インスタンスで設定されているトランスポート設定のヘッダー。	
	Type:	使用中の転送モード。 特定の転送モードでは、追加のフィールドが表示されます。たとえば、通信タイプが CSLU に設定されている場合、CSLU アドレスも表示されます。

フィールド	説明
ポリシー:	製品インスタンスに適用されるポリシー情報のヘッダー。
使用中のポリシー:	適用されるポリシー これは、Cisco default、Product default、Permanent License Reservation、Specific License Reservation、PAK license、Installed on <date>、Controller のいずれかです。
ポリシー名:	ポリシーの名前
レポートの ACK が必要:	この製品インスタンスのレポートに CSSM 確認応答 (ACK) が必要かどうかを指定する <i>yes</i> または <i>no</i> の値。デフォルトポリシーは常に「yes」に設定されます。
Unenforced/Non-Export Perpetual 属性	永久ライセンスのポリシー値を表示します。 <ul style="list-style-type: none"> 最初のレポート要件 (日): 最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 レポート頻度 (日): 次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 変化レポート (日): ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
Unenforced/Non-Export Subscription 属性	サブスクリプションライセンスのポリシー値を表示します。 <ul style="list-style-type: none"> 最初のレポート要件 (日): 最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 レポート頻度 (日): 次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 変化レポート (日): ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
Enforced (Perpetual/Subscription) ライセンス属性	

フィールド		説明
		<p>適用されたライセンスのポリシー値を表示します。</p> <ul style="list-style-type: none"> 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
	Export (Perpetual/Subscription) ライセンス属性	<p>輸出規制ライセンスのポリシー値を表示します。</p> <ul style="list-style-type: none"> 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
その他	カスタム ID のヘッダー。	
	カスタム ID:	ID

フィールド	説明
使用状況レポート:	使用状況レポート (RUM レポート) 情報のヘッダー。
最後に受信した ACK:	最後に受信した ACK の日時 (ローカルタイムゾーン)。
次の ACK 期限:	次の ACK の日時。ACK が不要であることがポリシーで示されている場合、このフィールドには <code>none</code> と表示されます。 Note ACK が必要で、この期限までに受信されない場合、 <code>syslog</code> が表示されます。
レポート間隔:	日単位のレポート間隔 ここに表示される値は、 license smart usage intervalinterval_in_days とポリシー値の設定によって異なります。詳細については、 Table 162: ポリシーを使用したスマートライセンスの show license status のフィールドの説明, on page 1829 で対応する構文の説明を参照してください。
次の ACK プッシュチェック:	製品インスタンスが ACK の次のポーリング要求を送信する日時。日時はローカルタイムゾーンで表示されます。 これは、CSSM または CSLU への製品インスタンスによって開始された通信にのみ適用されます。レポート間隔がゼロの場合、または ACK ポーリングが保留されていない場合、このフィールドには <code>none</code> と表示されます。
次のレポートプッシュ:	製品インスタンスが次の RUM レポートを送信する日時。日時はローカルタイムゾーンで表示されます。レポート間隔がゼロの場合、または保留中の RUM レポートがない場合、このフィールドには <code>none</code> と表示されます。
最後のレポートプッシュ:	製品インスタンスが最後の RUM レポートを送信した日時。日時はローカルタイムゾーンで表示されます。
最後のレポートファイル書き込み:	製品インスタンスが最後にオフライン RUM レポートを保存した日時。日時はローカルタイムゾーンで表示されます。
最後のレポートモデル:	データモデルを使用して使用状況レポート情報が取得された日時。日時はローカルタイムゾーンで表示されます。

フィールド	説明
インストール済み の信頼コード:	信頼コード関連情報のヘッダー。 信頼コードがインストールされている場合は、日時が表示されます。日時はローカルタイムゾーンで表示されます。 信頼コードがインストールされていない場合、このフィールドにはnoneと表示されます。
Active:	アクティブ製品インスタンス。 高可用性セットアップでは、セットアップ内のすべての製品インスタンスのUDIと、対応する信頼コードのインストール日時が表示されます。
Standby:	スタンバイ製品インスタンス。
Member:	メンバー製品インスタンス。

ポリシーを使用したスマートライセンスの show license status

次に、**show license status** コマンドの出力例を示します。（複数のソースからマージされた）シスコのデフォルトポリシーが、Cisco Catalyst 9500 スイッチに適用されます。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license status
Utility:
  Status: DISABLED
License Reservation is ENABLED
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
    Version privacy: DISABLED
Transport:
  Type: Transport Off
Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
```

```
Miscellaneous:
  Custom Id: <empty>
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Nov 29 10:50:05 2020 PDT
  Reporting Interval: 30
  Next ACK push check: <none>
  Next report push: Aug 31 10:52:05 2020 PDT
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
```

スマートライセンスの show license status

次に、**show license status** コマンドの出力例を示します。

```
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Initial Registration: First Attempt Pending
  Last Renewal Attempt: SUCCEEDED on Jul 19 14:49:49 2018 IST
  Next Renewal Attempt: Jan 15 14:49:47 2019 IST
  Registration Expires: Jul 19 14:43:47 2019 IST

License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST
  Last Communication Attempt: SUCCEEDED on Jul 28 07:02:56 2018 IST
  Next Communication Attempt: Aug 27 07:02:56 2018 IST
  Communication Deadline: Oct 26 06:57:50 2018 IST
```

Related Commands

コマンド	説明
show license all	権限付与情報を表示します。
show license authorization	許可コード関連情報を表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。

コマンド	説明
show tech-support license	デバッグ出力を表示します。

show license summary

使用されているライセンス、カウント、およびステータスに関する情報を含む、ライセンス使用状況の概要を表示するには、特権 EXEC モードで **show license summary** コマンドを使用します。

show license summary

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	<p>コマンド出力が更新され、ポリシーを使用したスマートライセンスの有効なライセンスステータスが反映されました。有効なライセンスステータスは、IN USE、NOT IN USE、NOT AUTHORIZED のみにになりました。</p> <p>コマンド出力が更新され、登録および承認情報が削除されました。</p> <p>コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。</p>

Usage Guidelines

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチのライセンスは、いずれも輸出規制または強制されていないため、NOT AUTHORIZED や NOT IN USE になることはありません（これらのライセンスのみ、使用する前に許可が必要です）。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールド（すべてのアクティブなライセンスの概要）が表示されます。

例

ディスプレイに表示されるフィールドについては、[Table 163: ポリシーを使用したスマートライセンスの show license summary のフィールドの説明, on page 1838](#) を参照してください。

ポリシーを使用したスマートライセンスの **show license summary**（Cisco Catalyst 9300 シリーズスイッチ）, [on page 1838](#)

ポリシーを使用したスマートライセンスの `show license summary` (Cisco Catalyst 9500 シリーズ スイッチ), on page 1838

`show license summary for Smart Licensing`, on page 1839

Table 163: ポリシーを使用したスマートライセンスの `show license summary` のフィールドの説明

フィールド	説明
License	使用中のライセンスの名前
Entitlement Tag	ライセンスの短縮名
Count	ライセンス数
Status	<p>ライセンスのステータスは次のいずれかになります。</p> <ul style="list-style-type: none"> • In-Use: 有効なライセンスかつ使用中。 • Not In-Use • Not Authorized: ライセンスを使用する前に Smart Licensing Authorization Code のインストールが必要であることを意味します。 (Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチには適用されません)

ポリシーを使用したスマートライセンスの `show license summary` (Cisco Catalyst 9300 シリーズ スイッチ)

次に、Cisco Catalyst 9300 スイッチでの `show license summary` コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license summary
```

```
License Usage:
License           Entitlement Tag           Count Status
-----
network-essentials (C9300-24 Network Essen...) 2 IN USE
dna-essentials    (C9300-24 DNA Essentials) 2 IN USE
network-essentials (C9300-48 Network Essen...) 1 IN USE
dna-essentials    (C9300-48 DNA Essentials) 1 IN USE
```

ポリシーを使用したスマートライセンスの `show license summary` (Cisco Catalyst 9500 シリーズ スイッチ)

次に、Cisco Catalyst 9500 スイッチでの `show license summary` コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license summary
```

```
License Usage:
License           Entitlement tag           Count Status
```

```
-----
network-advantage (C9500 Network Advantage)      2 IN USE
dna-advantage     (C9500-16X DNA Advantage)       2 IN USE
```

show license summary for Smart Licensing

次に、**show license summary** コマンドの出力例を示します。

```
Device# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: CISCO Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: SUCCEEDED
  Next Renewal Attempt: Jan 15 14:49:48 2019 IST

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 27 07:02:56 2018 IST

License Usage:
  License                               Entitlement tag                Count Status
  -----
  C9200L DNA Advantage... (C9200L-DNA-A-48)      1 AUTHORIZED
  C9200L Network Advan... (C9200L-NW-A-48)       1 AUTHORIZED
```

Related Commands

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。
show tech-support license	デバッグ出力を表示します。

show license tech

テクニカルサポートチームが問題をトラブルシューティングするのに役立つライセンス情報を表示するには、特権 EXEC モードで **show license tech** コマンドを入力します。このコマンドの出力には、他のいくつかの **show license** コマンドの出力などが含まれます。

show license tech { **data conversion** | **eventlog** [*days*] | **reservation** | **support** }

Syntax Description

data conversion ライセンスデータ変換情報を表示します。

eventlog [*days*] ポリシーを使用したスマートライセンスに関連するイベントログを表示します。

days には、イベントログを表示する日数を入力します。0 ~ 2147483647 の範囲の値を指定できます。

このオプションの出力は、**show license eventlog** コマンドと同じです。

reservation ライセンス予約情報を表示します。

support テクニカルサポートチームが問題をデバッグするのに役立つライセンス情報を表示します。

Command Modes

特権 EXEC (Device#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。

Usage Guidelines

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージとともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されず（スマートライセンスが有効になっているかどうか、関連するすべてのライセンス証明書、コンプライアンスステータスなど）。

ポリシーを使用したスマートライセンスの **show license tech support**

次に、Cisco Catalyst 9500 スイッチでの **show license tech support** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license tech support
Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 27 09:49:33 2021 PST
  Reporting push interval: 30 days State(2) InPolicy(90)
  Next ACK push check: <none>
```

```
Next report push: Oct 29 09:51:33 2020 PST
Last report push: <none>
Last report file write: <none>
```

License Usage

=====

Handle: 1

```
License: network-advantage
Entitlement Tag:
regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
Description: network-advantage
Count: 2
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 09:48:54 2020 PST
Request Time: Oct 29 09:49:18 2020 PST
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: network-advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 2
  Soft Enforced: True
```

Handle: 2

```
License: dna-advantage
Entitlement Tag:
regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
Description: C9500-16X DNA Advantage
Count: 2
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 09:48:54 2020 PST
Request Time: Oct 29 09:49:18 2020 PST
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9500-16X DNA Advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 2
  Soft Enforced: True
```

Handle: 7

```
License: air-network-advantage
Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
Description: air-network-advantage
Count: 0
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 10:49:09 2020 PST
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-network-advantage
Feature Description: air-network-advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
  Soft Enforced: True
```

Handle: 8

```
License: air-dna-advantage
Entitlement Tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

Description: air-dna-advantage
Count: 0
Version: 1.0
Status: IN USE(15)
Status time: Oct 29 10:49:09 2020 PST
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-dna-advantage
Feature Description: air-dna-advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
  Soft Enforced: True

Product Information
=====
UDI: PID:C9500-16X,SN:FCW2233A5ZV

HA UDI List:
  Active:PID:C9500-16X,SN:FCW2233A5ZV
  Standby:PID:C9500-16X,SN:FCW2233A5ZY

Agent Version
=====
Smart Agent for Licensing: 5.0.5_rel/42

Upcoming Scheduled Jobs
=====
Current time: Oct 29 11:04:46 2020 PST
Daily: Oct 30 09:48:56 2020 PST (22 hours, 44 minutes, 10 seconds remaining)
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Nov 05 09:52:25 2020 PST (6
days, 22 hours, 47 minutes, 39 seconds remaining)
Start Utility Measurements: Oct 29 11:19:09 2020 PST (14 minutes, 23 seconds remaining)
Send Utility RUM reports: Oct 30 09:53:10 2020 PST (22 hours, 48 minutes, 24 seconds
remaining)
Save unreported RUM Reports: Oct 29 12:04:19 2020 PST (59 minutes, 33 seconds remaining)
Process Utility RUM reports: Oct 30 09:49:33 2020 PST (22 hours, 44 minutes, 47 seconds
remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Nov 28 09:49:33 2020 PST (29 days, 22 hours, 44 minutes, 47 seconds remaining)
Operational Model: Expired Not Rescheduled

Communication Statistics:
=====
Communication Level Allowed: INDIRECT
Overall State: <empty>
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0   Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
```

```
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Result Polling:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Authorization Request:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Authorization Confirmation:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Authorization Return:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trust Sync:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Hello Message:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>

License Certificates
=====
Production Cert: True
Not registered. No certificates installed

HA Info
=====
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
=====
License reservation: ENABLED

Overall status:
Active: PID:C9500-16X,SN:FCW2233A5ZV
Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
```

```
Request code: <none>
Last return code: <none>
Last Confirmation code: 184ba6d6
Reservation authorization code:
Network Advantage</displayName><tagDescription>C9500 Network

Standby: PID:C9500-16X,SN:FCW2233A5ZY
Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
Request code: <none>
Last return code: <none>
Last Confirmation code: 961d598f
Reservation authorization code:
Network Advantage</displayName><tagDescription>C9500 Network

Specified license reservations:
C9500 Network Advantage (C9500 Network Advantage):
Description: C9500 Network Advantage
Total reserved count: 2
Enforcement type: NOT ENFORCED
Term information:
Active: PID:C9500-16X,SN:FCW2233A5ZV
Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
License type: PERPETUAL
Start Date: <none>
End Date: <none>
Term Count: 1
Subscription ID: <none>
Standby: PID:C9500-16X,SN:FCW2233A5ZY
Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
License type: PERPETUAL
Start Date: <none>
End Date: <none>
Term Count: 1
Subscription ID: <none>
C9500-DNA-16X-A (C9500-16X DNA Advantage):
Description: C9500-DNA-16X-A
Total reserved count: 2
Enforcement type: NOT ENFORCED
Term information:
Active: PID:C9500-16X,SN:FCW2233A5ZV
Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
License type: PERPETUAL
Start Date: <none>
End Date: <none>
Term Count: 1
Subscription ID: <none>
Standby: PID:C9500-16X,SN:FCW2233A5ZY
Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
License type: PERPETUAL
Start Date: <none>
End Date: <none>
Term Count: 1
Subscription ID: <none>

Purchased Licenses:
No Purchase Information Available

Other Info
```

```
=====
Software ID: regid.2017-05.com.cisco.C9500,v1_7435cf27-0075-4bfb-b67c-b42f3054e82a
Agent State: authorized
TS enable: True
Transport: Transport Off
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char) : 1
sizeof(int) : 4
sizeof(long) : 4
sizeof(char *) : 8
sizeof(time_t) : 4
sizeof(size_t) : 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPuginMgmtInterfaceMutex: True
SAPuginMgmtIPDomainName: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmRetrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: False
SmartTransportProxySupport: False
SmartAgentMaxRunMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
```

```
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: SmartAgentSystemDataListChanged
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 109 KB
P:C9500-16X,S:FCW2233A5ZV: No Trust Data
P:C9500-16X,S:FCW2233A5ZY: No Trust Data
Overall Trust: No ID
```

Platform Provided Mapping Table

=====

C9500-16X: Total licenses found: 143

Enforced Licenses:

P:C9500-16X,S:FCW2233A5ZV:

No PD enforced licenses

P:C9500-16X,S:FCW2233A5ZY:

No PD enforced licenses

show license udi

製品インスタンスの Unique Device Identifier (UDI) 情報を表示するには、特権 EXEC モードで **show license udi** コマンドを入力します。高可用性セットアップでは、接続されたすべての製品インスタンスの UDI 情報が出力に表示されます。

show license udi

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、ポリシーを使用したスマートライセンスの環境で引き続き使用できます。

Usage Guidelines **ポリシーを使用したスマートライセンス:** デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されません。

例

ポリシーを使用したスマートライセンスの [show licensing udi, on page 1848](#)

スマートライセンスの [show license udi, on page 1848](#)

ポリシーを使用したスマートライセンスの show licensing udi

次に、Catalyst 9500 スイッチでのハイアベイラビリティ設定の **show license udi** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license udi

UDI: PID:C9500-16X, SN:FCW2233A5ZV
HA UDI List:
Active:PID:C9500-16X, SN:FCW2233A5ZV
Standby:PID:C9500-16X, SN:FCW2233A5ZY
```

スマートライセンスの show license udi

次に、**show license udi** コマンドの出力例を示します。

```
Device# show license udi
UDI: PID:C9200L-48P-4X,SN:JPG221300KP
```

show license usage

ステータス、使用中のライセンス数、適用タイプなどのライセンス使用状況の情報を表示するには、特権 EXEC モードで **show license usage** コマンドを入力します。

show license usage

このコマンドには引数またはキーワードはありません。

Command Default

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。これには、 <code>Status</code> 、 <code>Enforcement type</code> フィールドが含まれます。 コマンド出力が更新され、予約関連情報、承認ステータス情報、および輸出ステータス情報が削除されました。

Usage Guidelines

ポリシーを使用したスマートライセンス: デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス: デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されません。

例

ディスプレイに表示されるフィールドについては、[Table 164: ポリシーを使用したスマートライセンス用 show license usage のフィールドの説明, on page 1850](#) を参照してください。

[ポリシーを使用したスマートライセンスの show license usage, on page 1852](#)

[スマートライセンスの show license usage, on page 1852](#)

Table 164: ポリシーを使用したスマートライセンス用 *show license usage* のフィールドの説明

フィールド	説明
License Authorization: Status:	全体的な承認ステータスを表示します。

フィールド	説明
():	CSSM におけるようなライセンスの名前。 このライセンスが承認コードを必要とする場合、ライセンスの取得されます。
説明	CSSM におけるようなライセンスの説明。
Count	ライセンス数。ライセンスが使用中でない場合、カウントはゼロになります。
Version	バージョン。
Status	ライセンスのステータスは次のいずれかになります。 <ul style="list-style-type: none"> • In-Use: 有効なライセンスかつ使用中。 • Not In-Use • Not Authorized: ライセンスを使用する前に SLAC のインストールを完了することを意味します。詳細については、次を参照してください。
Export Status:	このライセンスが輸出規制されているかどうかを示します。ステータスのいずれかが表示されます。 <ul style="list-style-type: none"> • RESTRICTED - ALLOWED • RESTRICTED - NOT ALLOWED • NOT RESTRICTED
Feature name	このライセンスを使用する機能の名前。
Feature Description:	このライセンスを使用する機能の説明。
ユーティリティのサブスクリプションID:	ID 対応する設定オプションがサポートされていないため、該当する機能は表示されません。
Enforcement type	ライセンスの適用タイプのステータス。これは、次のいずれかになります。 <ul style="list-style-type: none"> • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED 適用タイプの詳細については、次を参照してください。 <link>

ポリシーを使用したスマートライセンスの show license usage

次に、Cisco Catalyst 9500 スイッチでの **show license usage** コマンドの出力例を示します。ここでは、不適用ライセンスを使用中です。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license usage
License Authorization:
  Status: Not Applicable
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
dna-advantage (C9500-16X DNA Advantage):
  Description: C9500-16X DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-16X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
```

スマートライセンスの show license usage

次に、**show license usage** コマンドの出力例を示します。

```
Device# show license usage
License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST

C9200L DNA Advantage, 48-port Term license (C9200L-DNA-A-48):
  Description: C9200L DNA Advantage, 48-port Term license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9200L Network Advantage, 48-port license (C9200L-NW-A-48):
  Description: C9200L Network Advantage, 48-port license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

Related Commands

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。

コマンド	説明
show license udi	UDI を表示します。
show tech-support license	デバッグ出力を表示します。

show mac address-table

MAC アドレステーブルを表示するには、**show mac address-table** コマンドを特権 EXEC モードで使用します。

```
show mac address-table [ address mac-addr [ interface type/number | vlan vlan-id ] | aging-time
[ routed-mac | vlan vlan-id ] | control-packet-learn | count [ summary | vlan vlan-id ] | [ dynamic
| secure | static ] [ address mac-addr ] [ interface type/number | vlan vlan-id ] | interface type/number
| learning [ vlan vlan-id ] | multicast [ count ] [ igmp-snooping | mld-snooping | user ] [ vlan
vlan-id ] | notification { change [ interface [ type/number ] ] | mac-move | threshold } | vlan
vlan-id ]
```

Syntax Description	
address <i>mac-addr</i>	(任意) 特定の MAC アドレスの MAC アドレス テーブルに関する情報を表示します。
interface <i>type/number</i>	(任意) 特定のインターフェイスのアドレスを表示します。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のアドレスを表示します。
aging-time [routed-mac vlan <i>vlan-id</i>]	(任意) ルーテッド MAC または VLAN のエージングタイムを表示します。
control-packet-learn	(任意) 制御パケットの MAC 学習パラメータを表示します。
count	(任意) MAC アドレス テーブル内の現在のエントリ数を表示します。
dynamic	(任意) ダイナミックアドレスのみを表示します。
secure	(任意) セキュア アドレスだけを表示します。
static	(任意) スタティックアドレスのみを表示します。
learning	(任意) VLAN またはインターフェイスの学習を表示します。
multicast	(任意) マルチキャスト MAC アドレス テーブル エントリだけに関する情報を表示します。
igmp-snooping	(任意) Internet Group Management Protocol (IGMP) スヌーピングによって学習されたアドレスを表示します。
mld-snooping	(任意) Multicast Listener Discover version 2 (MLDv2) スヌーピングによって学習されたアドレスを表示します。
user	(任意) 手動で入力した (スタティック) アドレスを表示します。
notification change	MAC 通知パラメータおよび履歴テーブルを表示します。

notification mac-move	MAC 移動通知ステータスを表示します。
notification threshold	連想メモリ (CAM) テーブル利用通知ステータスを表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
	Cisco IOS XE Gibraltar 16.12.4	シスコのソフトウェアデファインドアクセス (SD-Access) ソリューションに使用される MAC アドレスを表示するように show mac address-table vlan vlan-id コマンドが更新されました。

Usage Guidelines *mac-addr* の値は 48 ビットの MAC アドレスです。有効なフォーマットは H.H.H です。

interface-number 引数では、モジュールとポート番号を指定します。有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

次に、**show mac address-table** コマンドの出力例を示します。

```
Device# show mac address-table

                Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
All     0100.0ccc.cccc  STATIC   CPU
All     0100.0ccc.cccd  STATIC   CPU
All     0180.c200.0000  STATIC   CPU
All     0180.c200.0001  STATIC   CPU
All     0180.c200.0002  STATIC   CPU
All     0180.c200.0003  STATIC   CPU
All     0180.c200.0004  STATIC   CPU
All     0180.c200.0005  STATIC   CPU
All     0180.c200.0006  STATIC   CPU
All     0180.c200.0007  STATIC   CPU
All     0180.c200.0008  STATIC   CPU
All     0180.c200.0009  STATIC   CPU
All     0180.c200.000a  STATIC   CPU
All     0180.c200.000b  STATIC   CPU
All     0180.c200.000c  STATIC   CPU
All     0180.c200.000d  STATIC   CPU
All     0180.c200.000e  STATIC   CPU
All     0180.c200.000f  STATIC   CPU
All     0180.c200.0010  STATIC   CPU
All     0180.c200.0021  STATIC   CPU
All     ffff.ffff.ffff  STATIC   CPU
  1     780c.f0e1.1dc3  STATIC   V11
  51    0000.1111.2222  STATIC   V151
  51     780c.f0e1.1dc6  STATIC   V151
1021    0000.0c9f.f45c  STATIC   V11021
```

```

1021    0002.02cc.0002    STATIC    Gi6/0/2
1021    0002.02cc.0003    STATIC    Gi6/0/3
1021    0002.02cc.0004    STATIC    Gi6/0/4
1021    0002.02cc.0005    STATIC    Gi6/0/5
1021    0002.02cc.0006    STATIC    Gi6/0/6
1021    0002.02cc.0007    STATIC    Gi6/0/7
1021    0002.02cc.0008    STATIC    Gi6/0/8
1021    0002.02cc.0009    STATIC    Gi6/0/9
1021    0002.02cc.000a    STATIC    Gi6/0/10

```

<output truncated>

次に、特定の MAC アドレスの MAC アドレステーブルを表示する例を示します。

```
Device# show mac address-table address fc58.9a02.7382
```

```

                Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       fc58.9a02.7382   DYNAMIC   Tel/0/1
Total Mac Addresses for this criterion: 1

```

次に、特定の VLAN に現在設定されているエイジングタイムを表示する例を示します。

```
Device# show mac address-table aging-time vlan 1
```

```

Global Aging Time: 300
Vlan    Aging Time
----    -
1       300

```

次に、特定のインターフェイスの MAC アドレステーブルに関する情報を表示する例を示します。

```
Device# show mac address-table interface TenGigabitEthernet1/0/1
```

```

                Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       fc58.9a02.7382   DYNAMIC   Tel/0/1
Total Mac Addresses for this criterion: 1

```

次に、MAC 移動通知ステータスを表示する例を示します。

```
Device# show mac address-table notification mac-move
```

```
MAC Move Notification: Enabled
```

次に、CAM テーブル利用通知ステータスを表示する例を示します。

```
Device# show mac address-table notification threshold
```

```

      Status      limit      Interval
-----+-----+-----
enabled          50          120

```

次に、特定のインターフェイスのMAC通知パラメータと履歴テーブルを表示する例を示します。

```
Device# show mac address-table notification change interface tenGigabitEthernet1/0/1

MAC Notification Feature is Disabled on the switch
Interface                               MAC Added Trap MAC Removed Trap
-----                               -
TenGigabitEthernet1/0/1                 Disabled       Disabled
```

次に、特定のVLANのMACアドレステーブルに関する情報を表示する例を示します。



Note シスコのSD-Accessソリューションを使用している場合は、CP_LEARNタイプのMACアドレスが表示されます。

```
Device# show mac address-table vlan 1021

          Mac Address Table
-----

Vlan      Mac Address      Type      Ports
----      -
1021     0000.0c9f.f45c   STATIC    Vl1021
1021     0002.02cc.0002   STATIC    Gi6/0/2
1021     0002.02cc.0003   STATIC    Gi6/0/3
1021     0002.02cc.0004   STATIC    Gi6/0/4
1021     0002.02cc.0005   STATIC    Gi6/0/5
1021     0002.02cc.0006   STATIC    Gi6/0/6
1021     0002.02cc.0007   STATIC    Gi6/0/7
1021     0002.02cc.0008   STATIC    Gi6/0/8
1021     0002.02cc.0009   STATIC    Gi6/0/9
1021     0002.02cc.000a   STATIC    Gi6/0/10
1021     0002.02cc.000b   STATIC    Gi6/0/11
1021     0002.02cc.000c   STATIC    Gi6/0/12
1021     0002.02cc.000d   STATIC    Gi6/0/13
1021     0002.02cc.000e   STATIC    Gi6/0/14
1021     0002.02cc.000f   STATIC    Gi6/0/15
1021     0002.02cc.0010   STATIC    Gi6/0/16
1021     0002.02cc.0011   STATIC    Gi6/0/17
1021     0002.02cc.0012   STATIC    Gi6/0/18
1021     0002.02cc.0013   STATIC    Gi6/0/19
1021     0002.02cc.0014   STATIC    Gi6/0/20

.
.
.

1021     0002.0100.0001   CP_LEARN  Tu0
1021     0002.0100.0002   CP_LEARN  Tu0
1021     0002.0100.0003   CP_LEARN  Tu0
1021     0002.0100.0004   CP_LEARN  Tu0
1021     0002.0100.0005   CP_LEARN  Tu0
1021     0002.0100.0006   CP_LEARN  Tu0
1021     0002.0100.0007   CP_LEARN  Tu0
1021     0002.0100.0008   CP_LEARN  Tu0
1021     0002.0100.0009   CP_LEARN  Tu0
1021     0002.0100.000a   CP_LEARN  Tu0
Total Mac Addresses for this criterion: 114
```

次の表で、**show mac address-table** の出力に表示される重要なフィールドを説明します。

Table 165: show mac address-table フィールドの説明

フィールド	説明
VLAN	VLAN 番号。
Mac Address	エントリの MAC アドレス。
タイプ	アドレスのタイプ。
ポート	ポート タイプ。
Total MAC addresses	MAC アドレステーブルの合計 MAC アドレス数。

Related Commands

コマンド	説明
clear mac address-table	MAC アドレス テーブルからダイナミック エントリを削除します。

show mac address-table move update

デバイス上の MAC アドレステーブル移動更新情報を表示するには、EXEC モードで **show mac address-table move update** コマンドを使用します。

show mac address-table move update

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default デフォルトの動作や値はありません。

Command Modes ユーザ EXEC

特権 EXEC

Command History リリース

Cisco IOS XE Fuji 16.9.2

例

次に、**show mac address-table move update** コマンドの出力例を示します。

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show parser encrypt file status

プライベート設定の暗号化ステータスを表示するには、**show parser encrypt file status** コマンドを使用します。

show parser encrypt file status

Syntax Description このコマンドには引数またはキーワードはありません。

Command Default なし

Command Modes ユーザ EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次のコマンド出力は、機能が使用可能で、ファイルが暗号化されていることを示します。ファイルは「暗号テキスト」形式です。

```
Device> enable
Device# show parser encrypt file status
Feature:                Enabled
File Format:            Cipher text
Encryption Version:    ver1
```

Related Commands

コマンド	説明
service private-config-encryption	プライベート設定ファイルの暗号化を有効にします。

show platform integrity

起動段階のチェックサムレコードを表示するには、特権 EXEC モードで **show platform integrity** コマンドを使用します。

```
show platform integrity [sign [nonce <nonce>]]
```

Syntax Description

sign	(任意) 署名を表示します。
nonce	(任意) ナンス値を入力します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
------	------

このコマンドが導入されました。

Examples

次に、起動段階のチェックサムレコードを表示する例を示します。

```
Device# show platform integrity sign

PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

show platform software audit

SE Linux 監査ログを表示するには、特権 EXEC モードで **show platform software audit** コマンドを使用します。

```
show platform software audit {all | summary | [switch {switch-number | active | standby}]
{0 | F0 | R0 | {FP | RP} {active}}}
```

Syntax Description	all	すべてのスロットからの監査ログを表示します。
	summary	すべてのスロットからの監査ログの要約カウントを表示します。
	switch	特定のスイッチのスロットについての監査ログを表示します。
	switch-number	指定したスイッチ番号のスイッチを選択します。
	switch active	スイッチのアクティブインスタンスを選択します。
	standby	スイッチのスタンバイインスタンスを選択します。
	0	SPA インターフェイス プロセッサ スロット 0 の監査ログを表示します。
	F0	Embedded-Service-Processor スロット 0 の監査ログを表示します。
	R0	Route-Processor スロット 0 の監査ログを表示します。
	FP active	アクティブな Embedded-Service-Processor スロットの監査ログを表示します。
	RP active	アクティブな Route-Processor スロットの監査ログを表示します。

Command Modes 特権 EXEC (#)

Command History

Usage Guidelines このコマンドは、Cisco IOS XE Gibraltar 16.10.1 で SELinux 許可モード機能の一部として導入されました。**show platform software audit** コマンドは、アクセス違反イベントを含むシステム ログを表示します。

Cisco IOS XE Gibraltar 16.10.1 では、許可モードでの操作は、IOS XE プラットフォームの特定のコンポーネント（プロセスまたはアプリケーション）を制限する目的で利用できます。許可モードでは、アクセス違反イベントが検出され、システム ログが生成されますが、イベントまたは操作自体はブロックされません。このソリューションは、主にアクセス違反検出モードで動作します。

次に、**show software platform software audit summary** コマンドの出力例を示します。

```
Device# show software platform software audit summary
```

```
=====
AUDIT LOG ON switch 1
-----
AVC Denial count: 58
=====
```

次に、**show software platform software audit all** コマンドの出力例を示します。

```
Device# show software platform software audit all
```

```
=====
AUDIT LOG ON switch 1
-----
===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc: denied { execute } for pid=8300 comm="sh"
name="id" dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438600.897:120): avc: denied { execute_no_trans } for pid=8300
comm="sh"
path="/tmp/sw/mount/cat9k-rpbase.2018-10-02_00.13_mhungund.SSA.pkg/nyquist/usr/bin/id"
dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438615.535:121): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
```

```

scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539440246.697:149): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539440299.119:150): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====

```

次に、**show software platform software audit switch** コマンドの出力例を示します。

```
Device# show platform software audit switch active R0
```

```

===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sdal" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0

```

```
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====
```

show platform software fed switch punt cause

インターフェイスで受信したパケットがルータプロセッサ（RP）にパントされている理由に関する情報を表示するには、特権 EXEC モードで **show platform software fed switch punt cpuq cause** コマンドを使用します。

show platform software fed switch *{switch-number | active | standby}* **punt** *{cause_id | clear | summary}*

Syntax Description

switch <i>{switch-number active standby}</i>	スイッチに関する情報を表示します。次の選択肢があります。 <ul style="list-style-type: none"> • <i>switch-number</i>。 • active : アクティブなスイッチに関する情報を表示します。 • standby: 存在する場合、スタンバイスイッチに関する情報を表示します。 <p>Note このキーワードはサポートされていません。</p>
<i>cause_id</i>	詳細を表示する必要がある原因の ID を指定します。
clear	すべての原因の統計をクリアします。原因をクリアすると、統計に矛盾が生じる可能性があります。
summary	パント理由の概要を表示します。

Command Default

なし

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines

なし

例

次に、**show platform software fed switch active punt cause summary** コマンドの出力例を示します。

```
Device# show platform software fed switch active punt cause summary
Statistics for all causes
```

Cause	Cause Info	Rcvd	Dropped
7	ARP request or response	1	0
21	RP<->QFP keepalive	22314	0

```
55    For-us control          12          0
60    IP subnet or broadcast packet  21          0
96    Layer2 control protocols 133808      0
-----
```

次に、**show platform software fed switch active punt cause** *cause-id* コマンドの出力例を示します。

```
Device# show platform software fed switch active punt cause 21
Detailed Statistics
```

```
Sub Cause      Rcvd          Dropped
-----
0              22363         0
-----
```

show platform software fed switch punt cpuq

CPU キューのパントラフィックに関する情報を表示するには、特権 EXEC モードで **show platform software fed switch punt cpuq** コマンドを使用します。

```
show platform software fed switch {switch-number | active | standby} punt cpuq {cpuq_id | all | brief | clear | rates}
```

Syntax Description

switch {*switch-number* **active** **standby**}

スイッチに関する情報を表示します。次の選択肢があります。

- **switch-number**。
- **active** : アクティブなスイッチに関する情報を表示します。
- **standby**: 存在する場合、スタンバイスイッチに関する情報を表示します。

Note このキーワードはサポートされていません。

punt

パント情報を表示します。

cpuq

CPU 受信キューに関する情報を表示します。

cpuq_id

特定の CPU キューに固有の詳細を指定します。

all

すべての CPU キューの統計を表示します。

brief

受信およびドロップされたパントパケットの詳細など、すべてのキューの要約された統計を表示します。

clear

すべての CPU キューの統計をクリアします。CPU キューをクリアすると、統計に矛盾が生じる可能性があります。

rates

パケットのパントレートを表示します。

Command Default

なし

Command Modes

特権 EXEC (#)

Command History

リリース

変更内容

Cisco IOS XE ジブラルタル 16.10.1 このコマンドが導入されました。

Usage Guidelines

なし

例

次に、**show platform software fed switch active punt cpuq brief** コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq brief
```

```
Punt CPU Q Statistics Brief
```

Q no	Queue Name	Rx prev	Rx cur	Rx delta	Drop prev	Drop cur	Drop delta
0	CPU_Q_DOT1X_AUTH	0	0	0	0	0	0
1	CPU_Q_L2_CONTROL	0	6772	6772	0	0	0
2	CPU_Q_FORUS_TRAFFIC	0	0	0	0	0	0
3	CPU_Q_ICMP_GEN	0	0	0	0	0	0
4	CPU_Q_ROUTING_CONTROL	0	12	12	0	0	0
5	CPU_Q_FORUS_ADDR_RESOLUTION	0	1	1	0	0	0
6	CPU_Q_ICMP_REDIRECT	0	0	0	0	0	0
7	CPU_Q_INTER_FED_TRAFFIC	0	0	0	0	0	0
8	CPU_Q_L2LVX_CONTROL_PKT	0	0	0	0	0	0
9	CPU_Q_EWLC_CONTROL	0	0	0	0	0	0
10	CPU_Q_EWLC_DATA	0	0	0	0	0	0
11	CPU_Q_L2LVX_DATA_PKT	0	0	0	0	0	0
12	CPU_Q_BROADCAST	0	21	21	0	0	0
13	CPU_Q_LEARNING_CACHE_OVFL	0	0	0	0	0	0
14	CPU_Q_SW_FORWARDING	0	0	0	0	0	0
15	CPU_Q_TOPOLOGY_CONTROL	0	127300	127300	0	0	0
16	CPU_Q_PROTO_SNOOPING	0	0	0	0	0	0
17	CPU_Q_BFD_LOW_LATENCY	0	0	0	0	0	0
18	CPU_Q_TRANSIT_TRAFFIC	0	0	0	0	0	0
19	CPU_Q_RPF_FAILED	0	0	0	0	0	0
20	CPU_Q_MCAST_END_STATION_SERVICE	0	0	0	0	0	0
21	CPU_Q_LOGGING	0	0	0	0	0	0
22	CPU_Q_PUNT_WEBAUTH	0	0	0	0	0	0
23	CPU_Q_HIGH_RATE_APP	0	0	0	0	0	0
24	CPU_Q_EXCEPTION	0	0	0	0	0	0
25	CPU_Q_SYSTEM_CRITICAL	0	0	0	0	0	0
26	CPU_Q_NFL_SAMPLED_DATA	0	0	0	0	0	0
27	CPU_Q_LOW_LATENCY	0	0	0	0	0	0
28	CPU_Q_EGR_EXCEPTION	0	0	0	0	0	0
29	CPU_Q_FSS	0	0	0	0	0	0
30	CPU_Q_MCAST_DATA	0	0	0	0	0	0
31	CPU_Q_GOLD_PKT	0	0	0	0	0	0

次の表で、この出力に表示される重要なフィールドを説明します。

Table 166: show platform software fed switch active punt cpuq brief フィールドの説明

フィールド	説明
Q no	キューの ID。
Queue Name	キューの名前。
Rx	受信されたパケット数。
Drop	ドロップされたパケットの数

次に、**show platform software fed switch active punt cpuq cpuq_id** コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq 1
```

```
Punt CPU Q Statistics
```

```
=====
CPU Q Id                : 1
CPU Q Name              : CPU_Q_L2_CONTROL
Packets received from ASIC : 6774
Send to IOSd total attempts : 6774
Send to IOSd failed count  : 0
RX suspend count        : 0
RX unsuspend count      : 0
RX unsuspend send count  : 0
RX unsuspend send failed count : 0
RX consumed count       : 0
RX dropped count         : 0
RX non-active dropped count : 0
RX conversion failure dropped : 0
RX INTACK count         : 6761
RX packets dq'd after intack : 0
Active RxQ event        : 6761
RX spurious interrupt    : 0
```

```
Replenish Stats for all rxq:
```

```
-----
Number of replenish      : 61969
Number of replenish suspend : 0
Number of replenish un-suspend : 0
-----
```

show platform software sl-infra

トラブルシューティング情報を表示し、デバッグに関する情報を表示するには、特権 EXEC モードで **show platform software sl-infra** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングとデバッグに使用します。

```
show platform software sl-infra { all | current | debug | stored }
```

Syntax Description

all 現在の情報、デバッグ情報、および保存されている情報を表示します。

current 現在のライセンス関連情報を表示します。

debug デバッグを有効にします。

stored 製品インスタンスに保存されている情報を表示します。

Command Modes

特権 EXEC (Device#)

Command History

リリース	変更内容
------	------

Cisco IOS XE Amsterdam 17.3.2a	このコマンドが導入されました。
--------------------------------	-----------------

Usage Guidelines

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージとともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

show platform sudi certificate

特定の SUDI のチェックサムレコードを表示するには、特権 EXEC モードで **show platform sudi certificate** コマンドを使用します。

show platform sudi certificate [**sign** [**nonce** <nonce>]]

Syntax Description

sign (任意) 署名を表示します。

nonce (任意) ナンス値を入力します。

Command Modes

特権 EXEC (#)

Command History

リリース 変更内容
ス

このコマンドが導入されました。

Examples

次に、特定の SUDI のチェックサムレコードを表示する例を示します。

デバイス# **show platform sudi certificate**

```

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbjbyBSb290IENBIDIwNDgwGgEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUEIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWtSEWdovyD0My5jOAmahBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJsZr2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWLBvLdT6ZeYpzPEApk0E5tzivMW/VgpSdh
jWn0f84bcN5wGyDwbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg91
Eg6CTY5j/e/rmxxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUtOG/rksc35LtlgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUJ/PI
FR5umgIJFq0roIlGx9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXH0jgXkhLtv5M0hmBvrbW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18J0agxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyC81WhJDtSd9i7rp77rMKsSH0T8lasz
Bvt9YaretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
kxpUnwVvwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPCCAySgAwIBAgIKYQ1ufQAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbjbyBSb290IENBIDIwNDgw
HhcNMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQKExMRYwFAYDVQQKEw1DaXNjb
bzEVMBMGAlUEAxMMQUNUMiBTvURJIEENBMBIIBjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAM5l3THixA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbs1Zq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCpuX+a6tHF/qRu0iJ44mdeDYzo3qPCpxzprWJDPc1M4iYKHUMQmQmgmg+
xghHiooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXDgJl3oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXLtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABO4IBWjCCAVYwCwYDVR0PBAQD

```

```

AgHGMB0GA1UdDgQWBbRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDIqNqA0hjJodHRWoi8vd3d3
LmNpc2NvLmNvbS9zZW50cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBGRBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNH0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNmMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQKV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3VyYXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGAlUdEwEB/wQIMAYBAf8CAQAwdQYJ
KozThvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbmSjbi
ZHC/CcCl01Ju0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVlPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOwryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hy147d7cZR4DY4LIuFM2P1As8YyjoNpK/urSRI14WdIlpLr1nH7KND15618yfVP
0IFJZBGrooCRBjOSwFv8cpWcbmWdPaCQT2nwIjTfy8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIDhJCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBGNVBAoTBUNp
c2NvNmRUwEwYDVQQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI1WhcNMjUw
ODA2MDgwODI1WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNdhVViBTTjppG
RE8xOTMyWDAwQzEOMAwGA1UEChMFQ21zY28xGDAWBgNVBAsTD0FDVC0yIExpDGUg
U1VESTZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNdhVWjCCASIdQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eUl4HcSwjL4HO75qTj19C2BHG3ufce9ikkN
xwGXi8qg8vKxub9tRYRaJC5bP1Wmoq7+ZJtQA079xE4X14soNbkq5NaUhh7RBlwD
iRUJvTfCoZVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNaj
nC73UXXM/hc0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1XOa262ZSQRiAxmaH/KLC
K97ywyRbdJlxBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGAp2+s8E9hsHPBPMCDIsCAwEAAANvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEAAQVAgOg
NRMzQ2hpcE1EPVVZSk5ORmRRRlFvN1ZIVmxJRTlqZENBeU9DQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HahDHtts3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0geziytsCf728KGw1oGuosgVjNGOOahUELu4+F/My7bIJNBH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQTyBaOLAbxsHvutrX
ulVZ5sdqStWtKk09vKMaQjh7a8J/AmJi93jvzm69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vror5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----

```

show running-config

現在実行されている設定ファイルまたは特定のモジュールのレイヤ 2 VLAN、クラスマップ、インターフェイス、マップクラス、ポリシーマップ、または仮想回線（VC）クラスの設定の内容を表示するには、**show running-config** コマンドを特権 EXEC モードで使

show running-config [*options*]

Syntax Description

オプション（任意）出力のカスタマイズに使用されるキーワード。複数のキーワードを入力できま

す。

- **aaa** [**accounting** | **attribute** | **authentication** | **authorization** | **diameter** | **group** | **ldap** | **miscellaneous** | **radius-server** | **server** | **tacacs-server** | **user-name** | **username**]: AAA の設定を表示します。
 - **all**: デフォルトパラメータで設定されたコマンドを含むように出力を展開します。 **all** キーワードを使用しない場合、デフォルトパラメータで設定されたコマンドは出力に表示されません。
 - **bridge-domain** {**id** | **parameterized vlan**}: ブリッジドメインの実行中コンフィギュレーションを表示します。
 - **brief**: 認定データや暗号化されたフィルタの詳細なしで設定を表示します。
 - **class-map** [*name*] [**linenum**]: クラスマップ情報を表示します。
 - **cts** [**interface** | **policy-server** | **rbm-rbac** | **server** | **sxp**]: Cisco TrustSec の設定を表示します。
 - **deprecated**: 実行中コンフィギュレーションとともに廃止された設定を表示します。
 - **eap** {**method** | **profiles**}: EAP 方式の設定とプロファイルを表示します。
 - **flow** {**exporter** | **monitor** | **record**}: グローバルフローコンフィギュレーションコマンドを表示します。
 - **full**: 完全な設定を表示します。
 - **identity** {**policy** | **profile**}: アイデンティティプロファイルまたはポリシー情報を表示します。
-

- **interface type number**: インターフェイス固有の設定情報を表示します。**interface** キーワードを使用する場合は、インターフェイスタイプとインターフェイス番号（たとえば、**interface GigabitEthernet 1/0/1** など）を指定する必要があります。システムで使用できるインターフェイスを特定するには、**show run interface ?** コマンドを使用します。
- **ip dhcp pool [name]**: IPv4 DHCP プールの設定を表示します。
- **ipv6 dhcp pool [name]**: IPv6 DHCP プールの設定を表示します。
- **linenum [brief | full | partition]**: 出力の行番号を表示します。
- **map-class [atm | dialer | frame-relay] [name]**: マップクラス情報を表示します。
- **mdns-sd [gateway | location-group | service-definition | service-list | service-peer | service-policy]**: マルチキャスト DNS サービス検出 (mDNS-SD) の設定を表示します。
- **partition {access-list | class-map | common | global-cdp | interface | ip-as-path | ip-community | ip-prefix-list | ip-static-routes | line | policy-map | route-map | router | snmp | tacacs}**: パーティションに対応する設定を表示します。
- **policy-map [name] [linenum]**: ポリシーマップ情報を表示します。
- **switch number**: 指定したスイッチの設定を表示します。
- **view [full]**: 完全な実行中のコンフィギュレーションを表示可能にします。これは、通常、特定のビューにアクセスする権限がある設定コマンドのみを表示できるビューベースのユーザ向けです。
- **vlan [vlan-id]**: 特定の VLAN 情報を表示します。有効な値は 1 ~ 4094 です。
- **vrf [vrf-name]**: 仮想ルーティングおよび転送 (VRF) 対応設定のモジュール番号を表示します。

Command Default

デフォルトシンタックスの **show running-config** では、デフォルトパラメータを使用して設定されたコマンドを除き、実行中コンフィギュレーションの内容を表示します。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show running-config コマンドは、技術的には **more system:running-config** コマンドのコマンドエイリアス（代替シンタックスまたは置換シンタックス）です。より多くのコマンドを使用することを推奨しますが（プラットフォーム間で構造が統一されており、拡張可能なシンタックスであるため）、**show running-config** コマンドは、幅広く使用し、**show run** などのショートカットを入力できるように有効のままになっています。

show running-config interface コマンドは、複数のインターフェイスがある場合に特定のインターフェイスの設定を確認する際に役立ちます。

linenum キーワードを指定すると、行番号が出力に表示されます。このオプションは、非常に大規模な設定の特定の部分を識別するのに役立ちます。

オプションのキーワードの後にパイプ文字 (|) を含めることで、コマンドシンタックスに追加の出力修飾子を入力できます。たとえば、**show running-config interface GigabitEthernet 1/0/1 linenum | begin 3** などです。キーワードに使用可能な出力修飾子を表示するには、キーワードの後に **|?** を入力します。使用しているプラットフォームによって、*options* 引数のキーワードと引数は異なる場合があります。

show running-config all コマンドは、デフォルト設定や値を含めて、完全な設定情報を表示します。たとえば、Cisco Discovery Protocol（出力では CDP と省略）の保留時間の値がデフォルトの 180 に設定されているとします。

- **show running-config** コマンドではこの値が表示されません。
- **show running-config all** では `cdp holdtime 180` を出力します。

Cisco Discovery Protocol の保留時間をデフォルト以外の値（100 など）に変更すると、**show running-config** コマンドと **show running-config all** コマンドの出力は同じになります。つまり、設定したパラメータが出力されます。

show running-config コマンドは ACL 情報を表示します。出力から ACL 情報を除外するには、**show running | section exclude ip access | access list** コマンドを使用します。

Examples

次に、GigabitEthernet0/0 インターフェイスを設定する例を示します。フィールドの説明は自明です。

```
Device# show running-config interface gigabitEthernet0/0

Building configuration...

Current configuration : 130 bytes
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 10.5.20.10 255.255.0.0
 negotiation auto
 ntp broadcast
end
```

次に、コマンド出力に行番号を設定し、出力修飾子を使用して 10 行目から表示を開始する例を示します。フィールドの説明は自明です。

```
Device# show running-config linenum | begin 10

10 : boot-start-marker
11 : boot-end-marker
12 : !
13 : no logging buffered
14 : enable password #####
15 : !
16 : spe 1/0 1/7
17 : firmware location bootflash:mica-modem-pw.10.16.0.0.bin
```

```
18 : !
19 : !
20 : resource-pool disable
21 : !
22 : no aaa new-model
23 : ip subnet-zero
24 : ip domain name cisco.com
25 : ip name-server 172.16.11.48
26 : ip name-server 172.16.2.133
27 : !
28 : !
29 : isdn switch-type primary-5ess
30 : !
.
.
.
126 : end
```

show running-config コマンドの次の出力例では、**shape average** コマンドによって ATM のトラフィックシェーピングのオーバーヘッドアカウンティングが有効になっていることが示されています。BRAS-DSLAM のカプセル化タイプは **qinq** で、加入者回線のカプセル化タイプは ATM アダプテーション層 5 (AAL5) に基づき **snap-rbe** になります。フィールドの説明は自明です。

```
Device# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
```

次に、**show running-config class-map** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```
Device# show running-config class-map
Building configuration...

Current configuration : 2157 bytes
!
class-map match-any system-cpp-police-ewlc-control
  description EWLC Control
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic
class-map match-any system-cpp-default
  description EWLC Data, Inter FED Traffic
```

```

class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-high-rate-app
  description High Rate Applications
class-map match-any system-cpp-police-multicast
  description MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual OOB
...

```

次に、teletype (tty) 回線 2 が 2 番目のコアとの通信用に予約されている例を示します。

```

Device# show running

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
!
interface Ethernet0
 ip address 10.25.213.150 255.255.255.128
 no ip directed-broadcast
 no logging event link-status
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 10.25.213.129
ip classless

```

```

ip route 0.0.0.0 0.0.0.0 10.25.213.129
!
!
line con 0
  transport input none
line 1 6
  no exec
  transport input all
line 7
  no exec
  exec-timeout 300 0
  transport input all
line 8 9
  no exec
  transport input all
line 10
  no exec
  transport input all
  stopbits 1
line 11 12
  no exec
  transport input all
line 13
  no exec
  transport input all
  speed 115200
line 14 16
  no exec
  transport input all
line aux 0
line vty 0 4
  password cisco
  login
!
end

```

Related Commands

Command	Description
copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします (copy system:running-config nvram:startup-config コマンドのコマンドエイリアス)。
show startup-config	NVRAM の内容を表示するか (存在していて有効な場合)、または CONFIG_FILE 環境変数によって指定されている設定ファイルを表示します (more:nvram startup-config コマンドのコマンドエイリアス)。

show sdm prefer

特定の機能用のシステムリソースを最大にするために使用できるテンプレートに関する情報を表示するには、特権 EXEC モードで **show sdm prefer** コマンドを使用します。現在のテンプレートを表示するには、キーワードを指定せずにコマンドを使用します。

show sdm prefer [**advanced**]

Syntax Description	advanced (任意) 高度なテンプレートに関する情報を表示します。
---------------------------	---

Command Default	デフォルトの動作や値はありません。
------------------------	-------------------

Command Modes	特権 EXEC
----------------------	---------

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **sdm prefer** グローバル コンフィギュレーション コマンドを入力後にデバイスをリロードしていない場合、**show sdm prefer** 特権 EXEC コマンドでは、新しく設定されたテンプレートではなく現在使用中のテンプレートが表示されます。

各テンプレートで表示される番号は、各機能のリソースにおけるおおよその最大数になります。他に設定された機能の実際の数字にもよるため、実際の数字とは異なる場合があります。たとえば、デバイスに 16 を超えるルーテッドインターフェイス（サブネット VLAN）がある場合、デフォルトのテンプレートでは、可能なユニキャスト MAC アドレスの数は 6000 未満になることがあります。

例

次に、**show sdm prefer** コマンドの出力例を示します。

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
Number of VLANs:                               4094
Unicast MAC addresses:                          16384
Overflow Unicast MAC addresses:                 256
L2 Multicast entries:                           1024
L3 Multicast entries:                           1024
Overflow L3 Multicast entries:                  256
Directly connected routes:                     10240
Indirect routes:                                4096
Security Access Control Entries:                1664
QoS Access Control Entries:                     1024
Policy Based Routing ACEs:                      512
```

```
Netflow Input ACEs:                128
Netflow Output ACEs:               128
Flow SPAN ACEs:                    256
Tunnels:                            128
LISP Instance Mapping Entries:      256
Control Plane Entries:              512
Input Netflow flows:                8192
Output Netflow flows:               8192
SGT/DGT (or) MPLS VPN entries:      2048
SGT/DGT (or) MPLS VPN Overflow entries: 256
Wired clients:                      2048
MACSec SPD Entries:                 128
```

These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

show tech-support confidential

show tech-support の機密情報を非表示にするには、特権 EXEC モードで **show tech-support confidential** コマンドを使用します。

show tech-support confidential output *file-name*

Syntax Description	output <i>file-name</i>	テクニカルサポートデータを保存する出力ファイルを指定します。
Command Default	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

Usage Guidelines **show tech-support confidential** コマンドは、MAC アドレス、IP アドレス、パスワードなどの機密データを非表示にします。出力は、すべての顧客固有のデータがマスクされた **show tech-support** コマンドの出力と同じです。

show tech-support confidential コマンドの出力は非常に長くなります。この出力を効率よく処理するには、**show tech-support confidential output location:filename** を使用してローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。

```
Device# show tech-support confidential output flash:tech_confidential
Collecting tech-support without confidential info, it will take few min..
```

リダイレクトされたファイルの出力を表示するには、**more location:filename** コマンドを使用します。

show tech-support license

デバッグ出力を表示するには、特権 EXEC モードで **show license tech support** コマンドを使用します。

show tech-support license

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show tech-support license** コマンドの出力例を示します。

```
Device# show tech-support license
----- show clock -----

*12:35:48.561 EDT Tue Jul 17 2018

----- show version -----

Cisco IOS XE Software, Version 16.09.01prd7
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.1prd7,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 10-Jul-18 08:47 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
!
!
!
```

Related Commands

コマンド	説明
show license all	権限付与情報を表示します。

コマンド	説明
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。

show tech-support monitor

SPAN モニタの情報を表示するには、特権 EXEC モードで **show tech-support monitor** コマンドを使用します。

show tech-support monitor [**switch** *switch-number* | **active** | **standby**]

Syntax Description		
	<i>switch-number</i>	スイッチを指定します。
	active	スイッチのアクティブインスタンスを指定します。
	standby	スイッチのスタンバイインスタンスを指定します。

Command Default	特権 EXEC (#)
------------------------	-------------

Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

Usage Guidelines **show tech-support monitor** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support monitor** [**switch** *switch-number* | **active** | **standby**] | **redirect location:filename**）。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。

リダイレクトされたファイルの出力を表示するには、**more location:filename** コマンドを使用します。

show tech-support platform

テクニカルサポートに使用するプラットフォームに関する詳細情報を表示するには、特権 EXEC モードで **show tech-support platform** コマンドを使用します。

show tech-support platform

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines

このコマンドは、プラットフォーム固有のデバッグに使用されます。出力には、CPU 使用率、Ternary Content Addressable Memory (TCAM) の使用率、容量、メモリ使用率など、プラットフォームに関する詳細情報が表示されます。

show tech-support platform コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform | redirect flash:filename**）。

show tech-support platform コマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なる場合があります。

Examples

次に、**show tech-support platform** コマンドの出力例を示します。

```
Device# show tech-support platform
.
.
.
----- show platform hardware capacity -----

Load Average
Slot Status 1-Min 5-Min 15-Min
1-RP0 Healthy 0.25 0.17 0.12

Memory (kB)
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
1-RP0 Healthy 3964428 2212476 (56%) 1751952 (44%) 3420472 (86%)

CPU Utilization
Slot CPU User System Nice Idle IRQ SIRQ IOwait
1-RP0 0 1.40 0.90 0.00 97.60 0.00 0.10 0.00
1 2.00 0.20 0.00 0.00 97.79 0.00 0.00 0.00
2 0.20 0.00 0.00 0.00 99.80 0.00 0.00 0.00
3 0.79 0.19 0.00 0.00 99.00 0.00 0.00 0.00
4 5.61 0.50 0.00 0.00 93.88 0.00 0.00 0.00
5 2.90 0.40 0.00 0.00 96.70 0.00 0.00 0.00
```

```

*: interface is up
IHQ: pkts in input hold queue      IQD: pkts dropped from input queue
OHQ: pkts in output hold queue     OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)           RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)           TXPS: tx rate (pkts/sec)
TRTL: throttle count

```

Interface	IHQ	IQD	OHQ	OQD	RXBS	RXPS
TXBS TXPS TRTL						
Vlan1	0	0	0	0	0	0
0 0 0						
* GigabitEthernet0/0	0	10179	0	0	2000	4
0 0 0						
GigabitEthernet1/0/1	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/2	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/3	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/4	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/5	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/6	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/7	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/8	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/9	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/10	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/11	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/12	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/13	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/14	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/15	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/16	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/17	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/18	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/19	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/20	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/21	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/22	0	0	0	0	0	0
0 0 0						
GigabitEthernet1/0/23	0	0	0	0	0	0
0 0 0						

show tech-support platform

```

GigabitEthernet1/0/24      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/25      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/26      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/27      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/28      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/29      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/30      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/31      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/32      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/33      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/34      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/35      0      0      0      0      0      0
0      0      0
GigabitEthernet1/0/36      0      0      0      0      0      0
0      0      0
Tel/0/37                    0      0      0      0      0      0
0      0      0
Tel/0/38                    0      0      0      0      0      0
0      0      0
Tel/0/39                    0      0      0      0      0      0
0      0      0
Tel/0/40                    0      0      0      0      0      0
0      0      0
Tel/0/41                    0      0      0      0      0      0
0      0      0
Tel/0/42                    0      0      0      0      0      0
0      0      0
Tel/0/43                    0      0      0      0      0      0
0      0      0
Tel/0/44                    0      0      0      0      0      0
0      0      0
Tel/0/45                    0      0      0      0      0      0
0      0      0
Tel/0/46                    0      0      0      0      0      0
0      0      0
Tel/0/47                    0      0      0      0      0      0
0      0      0
Tel/0/48                    0      0      0      0      0      0
0      0      0
Tel/1/1                     0      0      0      0      0      0
0      0      0
Tel/1/2                     0      0      0      0      0      0
0      0      0
Tel/1/3                     0      0      0      0      0      0
0      0      0
Tel/1/4                     0      0      0      0      0      0
0      0      0
ASIC 0 Info
-----
ASIC 0 HASH Table 0 Software info:  FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1

```

```

MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1
MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 1 Software info: FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1
MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1
MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 2 Software info: FSE 1
MAB 0: L3 Multicast entries srip 2 3
MAB 1: L3 Multicast entries srip 2 3
MAB 2: SGT_DGT          srip 0 1
MAB 3: SGT_DGT          srip 0 1
MAB 4: (null)           srip
MAB 5: (null)           srip
MAB 6: (null)           srip
MAB 7: (null)           srip
.
.
.

```

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
show tech-support platform evpn_vxlan	EVPN-VXLAN 関連のプラットフォーム情報を表示します。
show tech-support platform fabric	スイッチファブリックに関する詳細情報を表示します。
show tech-support platform igmp_snooping	グループに関する IGMP スヌーピング情報を表示します。
show tech-support platform layer3	レイヤ3 プラットフォーム転送情報を表示します。
show tech-support platform mld_snooping	グループに関する MLD スヌーピング情報を表示します。

show tech-support platform evpn_vxlan

テクニカルサポートに使用するイーサネット VPN (EVPN) Virtual Extensible LAN (VXLAN) 関連のプラットフォーム情報を表示するには、特権 EXEC モードで **show tech-support platform evpn_vxlan** コマンドを使用します。

show tech-support platform evpn_vxlan switch *switch-number*

Syntax Description	switch <i>switch-number</i>	指定されたスイッチに関する情報を表示します。有効な値は 1 ~ 9 です。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。
Usage Guidelines	このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、 show tech-support platform evpn_vxlan switch 1 redirect flash:filename ）。	

Examples

次に、**show tech-support platform evpn_vxlan** コマンドの出力例を示します。

```
Device# show tech-support platform evpn_vxlan switch 1
.
.
.
  "show clock"
  "show version"
  "show running-config"switch no: 1

----- sh sdm prefer -----

Showing SDM Template Info

This is the Advanced template.
Number of VLANs:                4094
Unicast MAC addresses:          32768
Overflow Unicast MAC addresses: 512
L2 Multicast entries:           4096
Overflow L2 Multicast entries:  512
L3 Multicast entries:           4096
Overflow L3 Multicast entries:  512
Directly connected routes:      16384
Indirect routes:                 7168
STP Instances:                   4096
Security Access Control Entries: 3072
QoS Access Control Entries:      2560
Policy Based Routing ACEs:       1024
Netflow ACEs:                    768
```

```

Flow SPAN ACEs:                512
Tunnels:                        256
LISP Instance Mapping Entries:  256
Control Plane Entries:         512
Input Netflow flows:           8192
Output Netflow flows:          16384
SGT/DGT (or) MPLS VPN entries: 4096
SGT/DGT (or) MPLS VPN Overflow entries: 512
Wired clients:                  2048
MACSec SPD Entries:            256
MPLS L3 VPN VRF:                127
MPLS Labels:                    2048
MPLS L3 VPN Routes VRF Mode:    7168
MPLS L3 VPN Routes Prefix Mode: 3072
MVPN MDT Tunnels:              256
L2 VPN EOMPLS Attachment Circuit: 256
MAX VPLS Bridge Domains :       64
MAX VPLS Peers Per Bridge Domain: 8
MAX VPLS/VPWS Pseudowires :    256

```

These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
* values can be modified by sdm cli.

```
----- show platform software fed switch 1 ifm interfaces nve -----
```

```
----- show platform software fed switch 1 ifm interfaces efp -----
```

```
----- show platform software fed switch 1 matm macTable -----
```

```

Total Mac number of addresses:: 0
*a_time=aging_time(secs) *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR          0x1  MAT_STATIC_ADDR          0x2  MAT_CPU_ADDR
  0x4  MAT_DISCARD_ADDR    0x8
MAT_ALL_VLANS              0x10 MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR
0x40  MAT_RESYNC           0x80
MAT_DO_NOT_AGE             0x100 MAT_SECURE_ADDR          0x200  MAT_NO_PORT
0x400  MAT_DROP_ADDR       0x800
MAT_DUP_ADDR               0x1000 MAT_NULL_DESTINATION     0x2000  MAT_DOT1X_ADDR
0x4000  MAT_ROUTER_ADDR    0x8000
MAT_WIRELESS_ADDR          0x10000 MAT_SECURE_CFG_ADDR      0x20000  MAT_OPQ_DATA_PRESENT
0x40000  MAT_WIRED_TUNNEL_ADDR 0x80000
MAT_DLR_ADDR               0x100000 MAT_MRP_ADDR              0x200000  MAT_MSRRP_ADDR
0x400000  MAT_LISP_LOCAL_ADDR 0x800000
MAT_LISP_REMOTE_ADDR      0x1000000 MAT_VPLS_ADDR             0x2000000
Device#

```

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform fabric

スイッチファブリックに関する情報を表示するには、特権 EXEC モードで **show tech-support platform fabric** コマンドを使用します。

```
show tech-support platform fabric [display-cli | vrf vrf-name {ipv4 display-cli | ipv6 display-cli |
source instance-id instance-id {ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix | mac mac-address}
{dest instance-id instance-id} {ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix | mac
mac-address} [display-cli]]
```

Syntax Description		
display-cli		(任意) このコマンドの出力で使用可能な show コマンドのリストを表示します。
vrf <i>vrf-name</i>		(任意) 指定した Virtual Routing and Forwarding (VRF) インスタンスのファブリック関連情報を表示します。
ipv4 <i>ip-address/ip-prefix</i>		(任意) 送信元または宛先 IPv4 VRF のファブリック関連情報を表示します。
ipv6 <i>ipv6-address/ipv6-prefix</i>		(任意) 送信元または宛先 IPv6 VRF のファブリック関連情報を表示します。
source		(任意) 送信元 VRF のファブリック関連情報を表示します。
instance-id <i>instance-id</i>		(任意) 送信元のエンドポイント識別子 (EID) に関する情報を表示します。
mac <i>mac-address</i>		(任意) レイヤ 2 拡張展開の送信元および宛先 MAC VRF のファブリック関連情報を表示します。
Command Modes	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Usage Guidelines

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform fabric | redirect flash:filename**）。

このコマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なる場合があります。

Examples

次に、**show tech-support platform fabric vrf source instance-id ipv4 dest instance-id ipv4** コマンドの出力例を示します。

```
Device# show tech-support platform fabric vrf DEFAULT_VN source instance-id
4098 ipv4 10.1.1.1/32 dest instance-id 4098 ipv4 10.12.12.12/32

.
.
.
-----show ip lisp eid-table vrf DEFAULT_VN forwarding eid remote 10.12.12.12-----

Prefix          Fwd action  Locator status bits  encap_iid
10.12.12.12/32  encap      0x00000001             N/A
  packets/bytes  1/576
  path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwc]
  ifnums:
    LISP0.4098 (78): 192.0.2.2
  1 path
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
      nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
  1 output chain
    chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
      IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378

-----show lisp instance-id 4098 ipv4 map-cache-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
10.1.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Locator Uptime   State      Pri/Wgt   Encap-IID
192.0.2.2 02:45:54 up         10/10    -

-----show lisp instance-id 4098 ipv4 map-cache detail-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 2(676 bytes) (~ 02:45:38 ago)
  Configured as EID address space
  Encapsulating to proxy ETR
101.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
```

```

State: send-map-request, last modified: 02:46:01, map-source: local
Exempt, Packets out: 0(0 bytes)
Configured as EID address space
Configured as dynamic-EID address space
Encapsulating dynamic-EID traffic
Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
Last RLOC-probe sent: 02:45:54 (rtt 1ms)

```

```
-----show lisp instance-id 4098 ipv4 map-cache 10.12.12.12/32-----
```

```

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
Last RLOC-probe sent: 02:45:54 (rtt 1ms)

```

```
-----show ip cef vrf DEFAULT_VN 10.12.12.12/32 internal-----
```

```

10.12.12.12/32, epoch 1, flags [sc, lisp elig], refcnt 6, per-destination sharing
sources: LISP, IPL
feature space:
Broker: linked, distributed at 1st priority
subblocks:
SC owned,sourced: LISP remote EID - locator status bits 0x00000001
LISP remote EID: 1 packets 576 bytes fwd action encap, cfg as EID space
LISP source path list
path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwc]
ifnums:
LISP0.4098(78): 192.0.2.2
1 path
path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
1 output chain
chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
Dependent covered prefix type LISP, cover 0.0.0.0/0
2 IPL sources [no flags]
ifnums:
LISP0.4098(78): 192.0.2.2
path list 7F44EEC2C188, 3 locks, per-destination, flags 0x49 [shble, rif, hwc]
path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4

```

show tech-support platform fabric

```

nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8

output chain:
  PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
  IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
  IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
switch no: 1
.
.
.

Device# show tech-support platform fabric vrf Campus_VN source instance-id 8189
mac 00b7.7128.00a1 dest instance-id 8189 mac 00b7.7128.00a0 | i show

----- show clock -----
----- show version -----
----- show running-config -----
----- show device-tracking database -----
----- show lisp site -----
----- show mac address-table address 00B7.7128.00A0-----
----- show ip arp vrf Campus_VN-----
Device#

```

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform igmp_snooping

グループに関する Internet Group Management Protocol (IGMP) スヌーピング情報を表示するには、特権 EXEC モードで **show tech-support platform igmp_snooping** コマンドを使用します。

show tech-support platform igmp_snooping [**Group_ipAddr** *ipv4-address* | [**vlan** *vlan-ID*]]

Syntax Description	Group_ipAddr	
		(任意) 指定したグループアドレスに関するスヌーピング情報を表示します。
	<i>ipv4-address</i>	(任意) グループの IPv4 アドレス。
	vlan <i>vlan-ID</i>	(任意) IGMP スヌーピング VLAN 情報を表示します。有効な値は 1 ~ 4094 です。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします (たとえば、**show tech-support platform igmp_snooping | redirect flash:filename**)。

Examples

次に、**show tech-support platform igmp_snooping** コマンドの出力例を示します。

```
Device# show tech-support platform igmp_snooping GroupIPAddr 226.6.6.6 vlan
.
.
.
----- show ip igmp snooping groups | i 226.6.6.6 -----
5          226.6.6.6          user          Gi1/0/8, Gi1/0/27, Gi1/0/28,

----- show ip igmp snooping groups count -----
Total number of groups:  2

----- show ip igmp snooping mrouter -----
```

show tech-support platform igmp_snooping

```
Vlan    ports
-----
    23    Router
    24    Router
    25    Router
```

```
----- show ip igmp snooping querier -----
```

Vlan	IP Address	IGMP Version	Port
23	10.1.1.1	v2	Router
24	10.1.2.1	v2	Router
25	10.1.3.1	v2	Router

```
----- show ip igmp snooping vlan 5 -----
```

```
Global IGMP Snooping configuration:
```

```
-----
IGMP snooping           : Enabled
Global PIM Snooping    : Disabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count  : 2
Robustness variable    : 2
Last member query count : 2
Last member query interval : 1000
```

```
Vlan 5:
```

```
-----
IGMP snooping           : Enabled
Pim Snooping           : Disabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable    : 2
Last member query count : 2
Last member query interval : 1000
```

```
----- show ip igmp snooping groups vlan 5 -----
```

Vlan	Group	Type	Version	Port List
5	226.6.6.6	user		Gi1/0/8, Gi1/0/27, Gi1/0/28, Gi2/0/7, Gi2/0/8, Gi2/0/27, Gi2/0/28
5	238.192.0.1	user		Gi2/0/28

```
----- show platform software fed active ip igmp snooping vlan 5 -----
```

```
Vlan 5
-----
```

```

IGMPSN Enabled : On
PIMSN Enabled  : Off
Flood Mode     : On
I-Mrouter      : Off
Oper State     : Up
STP TCN Flood  : Off
Routing Enabled: Off
PIM Enabled    : Off
PVLAN         : No
In Retry       : 0x0
L3mcast Adj    :
Mrouter PortQ  :
Flood PortQ   :

```

```
----- show platform software fed active ip igmp snooping groups | begin 226.6.6.6 -----
```

```
Vlan:5 Group:226.6.6.6
```

```

-----
Member ports      :
CAPWAP ports     :
Host Type Flags: 0
Failure Flags    : 0
DI handle        : 0x7f11151cbad8
REP RI handle    : 0x7f11151cc018
SI handle        : 0x7f11151cd198
HTM handle       : 0x7f11151cd518

```

```
si hdl : 0x7f11151cd198 rep ri hdl : 0x7f11151cc018 di hdl : 0x7f11151cbad8 htm hdl : 0x7f11151cd518
```

```

.
.
.

```

```
Device#
```

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
ip igmp snooping	IGMP スヌーピングをグローバルまたはインターフェイスで有効にします。
show ip igmp snooping	デバイスの IGMP スヌーピング設定を表示します。
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform layer3

レイヤ 3 プラットフォーム転送情報を表示するには、特権 EXEC モードで **show tech-support platform layer3** コマンドを使用します。

```
show tech-support platform layer3 {multicast Group_ipv6Addr ipv4-address switch switch-number srcIP
ipv4-address | unicast {dstIP ipv4-address srcIP ipv4-address | vrf vrf-name destIP ipv4-address srcIP
ipv4-address}}
```

Syntax Description		
multicast		マルチキャスト情報を表示します。
Group_ipv6Addr <i>ipv4-address</i>		指定したマルチキャスト グループアドレスに関する情報を表示します。
switch <i>switch-number</i>		指定したスイッチに関する情報を表示します。有効な値は 1 ～ 9 です。
srcIP <i>ipv4-address</i>		指定した送信元アドレスに関する情報を表示します。
unicast		ユニキャスト関連の情報を表示します。
dstIP <i>ipv4-address</i>		指定した宛先アドレスに関する情報を表示します。
vrf <i>vrf-name</i>		ユニキャスト関連の Virtual Routing and Forwarding (VRF) 情報を表示します。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform layer3 multicast group 224.1.1.1 switch 1 srcIP 10.10.0.2 | redirect flash:filename**）。

Examples

次に、**show tech-support platform layer3 multicast group** コマンドの出力例を示します。

```

Device# show tech-support platform layer3 multicast group_ipAddr 224.1.1.1
switch 1 srcIp 10.10.0.2

.
.
.
destination IP: 224.1.1.1
source IP: 10.10.0.2
switch no: 1

----- show ip mroute 224.1.1.1 10.10.0.2 -----

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.10.0.2, 224.1.1.1), 00:00:22/00:02:37, flags: LFT
  Incoming interface: GigabitEthernet1/0/10, RPF nbr 0.0.0.0, Registering
  Outgoing interface list:
    Vlan20, Forward/Sparse, 00:00:22/00:02:37, A

----- show ip mfib 224.1.1.1 10.10.0.2 -----

Entry Flags:   C - Directly Connected, S - Signal, IA - Inherit A flag,
               ET - Data Rate Exceeds Threshold, K - Keepalive
               DDE - Data Driven Event, HW - Hardware Installed
               ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
               MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
               MS - MoFRR Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:  FS Pkt Count/PS Pkt Count
Default
(10.10.0.2,224.1.1.1) Flags: HW
SW Forwarding: 0/0/0/0, Other: 1/1/0
HW Forwarding:  NA/NA/NA/NA, Other: NA/NA/NA
GigabitEthernet1/0/10 Flags: A
Vlan20 Flags: F IC
Pkts: 0/0
Tunnel0 Flags: F

```

show tech-support platform layer3

Pkts: 0/0

----- show platform software fed switch 1 ip multicast interface summary -----

Multicast Interface database

VRF	Interface SVI	IF ID	PIM Status	State	RI Handle
0	GigabitEthernet1/0/10	0x0000000000000005f	enabled	0x0000000000000010	
	0x00007fb414b1f108 false				
0	Vlan20	0x00000000000000060	enabled	0x0000000000000010	
	0x00007fb414b31a98 true				

----- show platform software fed switch 1 ip multicast groups summary -----

Multicast Groups database

Mvrf_id: 0 Mroute: (*, 224.0.1.40/32) Flags: C IC
Htm: 0x00007fb414b23ce8 Si: 0x00007fb414b23a08 Di: 0x00007fb414b240e8 Rep_ri:
0x00007fb414b245f8

Mvrf_id: 0 Mroute: (*, 224.0.0.0/4) Flags: C
Htm: 0x00007fb4143549e8 Si: 0x00007fb414b20a48 Di: 0x00007fb414b1fe78 Rep_ri:
0x00007fb414b20428

Mvrf_id: 0 Mroute: (*, 224.1.1.1/32) Flags: C IC
Htm: 0x00007fb414b2cc98 Si: 0x00007fb414b2b678 Di: 0x00007fb414b2ab98 Rep_ri:
0x00007fb414b2b0c8

Mvrf_id: 0 Mroute: (10.10.0.2, 224.1.1.1/32) Flags: IC
Htm: 0x00007fb414b2f348 Si: 0x00007fb414b321d8 Di: 0x00007fb414b2dba8 Rep_ri:
0x00007fb414b30ed8

----- show platform software fed switch 1 ip multicast groups count -----

Total Number of entries:4

----- show platform software fed switch 1 ip multicast groups 224.1.1.1/32
source 10.10.0.2 detail -----

MROUTE ENTRY vrf 0 (10.10.0.2, 224.1.1.1/32)
HW Handle: 140411418055080 Flags: IC
RPF interface: GigabitEthernet1/0/10(95)):
HW Handle:140411418055080 Flags:A
Number of OIF: 3
Flags: 0x4 Pkts : 0
OIF Details:
Tunnel0 Adj: 0xf8000636 F
Vlan20 Adj: 0xf8000601 F IC
GigabitEthernet1/0/10 A
Htm: 0x7fb414b2f348 Si: 0x7fb414b321d8 Di: 0x7fb414b2dba8 Rep_ri: 0x7fb414b30ed8

```

DI details
-----
Handle:0x7fb414b2dba8 Res-Type:ASIC_RSC_DI Res-Switch-Num:255 Asic-Num:255
Feature-ID:AL_FID_L3_
MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x538e
mtu_index/l3u_ri_index0:0x0 index1:0x538e mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----

Destination Index (DI) [0x538e]
portMap = 0x00000000          0
cmil = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
-----

Destination Index (DI) [0x538e]
portMap = 0x00000000          0
cmil = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0

=====

RI details
-----
Handle:0x7fb414b30ed8 Res-Type:ASIC_RSC_RI_REP Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x5 mtu_index/l3u_ri_index0:0x0
index1:0x5 mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

```

Detailed Resource Information (ASIC# 0)
-----

Detailed Resource Information (ASIC# 1)
-----

=====

SI details
-----
Handle:0x7fb414b321d8 Res-Type:ASIC_RSC_SI_STATS Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x4004 mtu_index/l3u_ri_index0:
0x0 sm handle 0:0x7fb414b2df98 index1:0x4004 mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----
Detailed Resource Information (ASIC# 1)
-----

=====

HTM details
-----
Handle:0x7fb414b2f348 Res-Type:ASIC_RSC_HASH_TCAM Res-Switch-Num:0 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_SG ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: handle0:0x7fb414b2f558
Detailed Resource Information (ASIC# 0)
-----
Number of HTM Entries: 1

Entry #0: (handle 0x7fb414b2f558)

KEY - src_addr:10.10.0.2 starg_station_index: 16387
MASK - src_addr:0.0.0.0 starg_station_index: 0
AD: use_starg_match: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0 rpf_valid: 1 rpf_le_ptr: 0

afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1 cpp_type: 0 dest_mod_index: 0
rp_index:
0 priority: 5 rpf_le: 36 station_index: 16388 capwap_mgid_present: 0 mgid 0

=====

次に、show tech-support platform layer3 unicast vrf コマンドの出力例を示します。

Device# show tech-support platform layer3 unicast vrf vr1 dstIP 10.0.0.20
srcIP 10.0.0.10

.
.
.
destination IP: 10.0.0.20
source IP: 10.0.0.10
vrf name :

Switch/Stack Mac Address : 5006.ab89.0280 - Local Mac Address
Mac persistency wait time: Indefinite

Switch#      Role      Mac Address      Priority Version  State
-----

```

```
*1      Active   5006.ab89.0280   1      V02      Ready

----- show switch -----

10.0.0.10 -> 10.0.0.20 =>IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20

----- show ip cef    exact-route platform  10.0.0.10 10.0.0.20 -----

nexthop is 10.0.0.20

Protocol Interface          Address
IP      GigabitEthernet1/0/7  10.0.0.20(8)
                                0 packets, 0 bytes
                                epoch 0
                                sourced in sev-epoch 0
                                Encap length 14
                                00211BFDE6495006AB8902C00800
                                L2 destination address byte offset 0
                                L2 destination address byte length 6
                                Link-type after encap: ip
                                ARP

----- show adjacency 10.0.0.20 detail -----

Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet1/0/7
    Route metric is 0, traffic share count is 1

----- show ip route  10.0.0.20 -----

10.0.0.20/32, epoch 3, flags [attached]
  Adj source: IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20 FF90E67820
  Dependent covered prefix type adjfib, cover 10.0.0.0/24
  attached to GigabitEthernet1/0/7

----- show ip cef  10.0.0.20 detail -----

ip prefix: 10.0.0.20/32

Forwarding Table

10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
```

```
Connected Interface: 31
Prefix Flags: Directly L2 attached
OM handle: 0x10205416d8
```

```
----- show platform software ip switch 1 R0 cef prefix 10.0.0.20/32 detail -----
```

```
OBJ_ADJACENCY found: 29
```

```
Number of adjacency objects: 5
```

```
Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  OM handle: 0x1020541348
```

```
----- show platform software adjacency switch 1 R0 index 29 -----
```

```
Forwarding Table
```

```
10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
Connected Interface: 31
Prefix Flags: Directly L2 attached
aom id: 393, HW handle: (nil) (created)
```

```
----- show platform software ip switch 1 F0 cef prefix 10.0.0.20/32 detail -----
```

```
OBJ_ADJACENCY found: 29
```

```
Number of adjacency objects: 5
```

```
Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  aom id: 391, HW handle: (nil) (created)
```

```
----- show platform software adjacency switch 1 F0 index 29 -----
```

```
found aom id: 391
```

```
Object identifier: 391
  Description: adj 0x1d, Flags None
  Status: Done, Epoch: 0, Client data: 0xc6a747a8
```

```
----- show platform software object-manager switch 1 F0 object 391 -----
```

```
Object identifier: 66
  Description: intf GigabitEthernet1/0/7, handle 31, hw handle 31, HW dirty: NONE AOM dirty
  NONE
  Status: Done
```

```
----- show platform software object-manager switch 1 F0 object 391 parents -----
```

```
Object identifier: 393
  Description: PREFIX 10.0.0.20/32 (Table id 0)
  Status: Done
```

```
.
.
.
```

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform mld_snooping

グループに関するマルチキャストリスナー検出（MLD）スヌーピング情報を表示するには、特権 EXEC モードで **show tech-support platform mld_snooping** コマンドを使用します。

show tech-support platform mld_snooping [**Group_ipv6Addr** *ipv6-address*][**vlan** *vlan-ID*]

Syntax Description	Group_ipv6Addr	
		(任意) 指定したグループアドレスに関するスヌーピング情報を表示します。
	<i>ipv6-address</i>	(任意) グループの IPv6 アドレス。
	vlan <i>vlan-ID</i>	(任意) MLD スヌーピング VLAN 情報を表示します。有効な値は 1 ~ 4094 です。

Command Modes 特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

Usage Guidelines このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform mld_snooping | redirect flash:filename**）。

Examples

次に、**show tech-support platform mld_snooping** コマンドの出力例を示します。

```
Device# show tech-support platform mld_snooping GroupIPv6Addr FF02::5:1
```

```
.
.
.
```

```
----- show running-config -----
```

```
Building configuration...
```

```
Current configuration : 11419 bytes
!
! Last configuration change at 09:17:04 UTC Thu Sep 6 2018
!
version 16.10
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
no platform punt-keepalive disable-kernel-core
!
```

```
hostname Switch
!
!
vrf definition Mgmt-vrf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
!
no aaa new-model
switch 1 provision ws-c3650-12x48uq
!
!
!
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "profile-1"
  active
  destination transport-method http
  no destination transport-method email
!
!
!
!
!
ip admission watch-list expiry-time 0
!
!
!
login on-success log
!
!
!
!
no device-tracking logging theft
!
crypto pki trustpoint TP-self-signed-559433368
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-559433368
  revocation-check none
  rsakeypair TP-self-signed-559433368
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-559433368
certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 35353934 33333336 38301E17 0D313531 32303331 32353432
  325A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3535 39343333
  33363830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  AD8C9C3B FEE7FFC8 986837D2 4C126172 446C3C53 E040F798 4BA61C97 7506FDCE
```

show tech-support platform mld_snooping

```

46365D0A E47E3F4F C774CA5B 73E2A8DD B72A2E98 C66DB196 94E8150F 0B669CF6
AA5BC4CD FC2E02F6 FE08B17F 0164FC19 7DC84ABB C99D91D6 398233FF 814EF6DA
6DC8FC20 CA12C0D6 1CB28EDA 6ADD6DFA 7E3E8281 4A189A9A AA44FCC0 BA9BD8A5
02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
23041830 16801448 668D668E C92914BB 69E9BA64 F61228DE 132E2030 1D060355
1D0E0416 04144866 8D668EC9 2914BB69 E9BA64F6 1228DE13 2E20300D 06092A86
4886F70D 01010505 00038181 0000F1D3 3DD1E5F1 EB714A95 D5819933 CAD0C943
59927D55 9D70CAD0 D64830EB D54380AD D2B5B613 F8AF7A5B 1F801134 246F760D
5E5515DB D098304F 5086F6CE 88E8B576 F6B93A88 F458FDCF 91A42D7E FA741908
5C892D78 600FB655 E6C5A4D0 6C1F1B9A 3AECA550 E3DC0881 01C4D004 7AB65BC3
88CF24DE DAA19474 51B535A5 0C
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
!
diagnostic bootup level minimal
diagnostic monitor syslog
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
redundancy
mode sso
!
!
!
!
!
!
class-map match-any system-cpp-police-topology-control
description Topology control
class-map match-any system-cpp-police-sw-forward
description Sw forwarding, L2 LVX data, LOGGING

```

```
class-map match-any system-cpp-default
  description EWLC control, EWLC data, Inter FED
class-map match-any system-cpp-police-sys-data
  description Learning cache ovfl, High Rate App, Exception, EGR Exception, NFL SAMPLED
  DATA, RPF Failed
class-map match-any AutoQos-4.0-RT1-Class
  match dscp ef
  match dscp cs6
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any AutoQos-4.0-RT2-Class
  match dscp cs4
  match dscp cs3
  match dscp af41
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-multicast
  description Transit Traffic and MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual
class-map match-any system-cpp-police-control-low-priority
  description ICMP redirect and general punt
class-map match-any system-cpp-police-wireless-priority1
  description Wireless priority 1
class-map match-any system-cpp-police-wireless-priority2
  description Wireless priority 2
class-map match-any system-cpp-police-wireless-priority3-4-5
  description Wireless priority 3,4 and 5
class-map match-any non-client-nrt-class
class-map match-any system-cpp-police-routing-control
  description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
  description Protocol snooping
class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
!
policy-map system-cpp-policy
  class system-cpp-police-data
    police rate 200 pps
  class system-cpp-police-routing-control
    police rate 500 pps
  class system-cpp-police-control-low-priority
  class system-cpp-police-wireless-priority1
  class system-cpp-police-wireless-priority2
  class system-cpp-police-wireless-priority3-4-5
policy-map port_child_policy
  class non-client-nrt-class
    bandwidth remaining ratio 10
!
!
!
!
```

```
!  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0  
  vrf forwarding Mgmt-vrf  
  no ip address  
  speed 1000  
  negotiation auto  
!  
interface GigabitEthernet1/0/1  
  switchport mode access  
  macsec network-link  
!  
interface GigabitEthernet1/0/2  
!  
interface GigabitEthernet1/0/3  
!  
interface TenGigabitEthernet1/1/1  
!  
interface TenGigabitEthernet1/1/2  
!  
interface TenGigabitEthernet1/1/3  
!  
interface TenGigabitEthernet1/1/4  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
ip forward-protocol nd  
ip http server  
ip http authentication local  
ip http secure-server  
!  
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data  
  permit tcp any any eq 22  
  permit tcp any any eq 465  
  permit tcp any any eq 143  
  permit tcp any any eq 993  
  permit tcp any any eq 995  
  permit tcp any any eq 1914  
  permit tcp any any eq ftp  
  permit tcp any any eq ftp-data  
  permit tcp any any eq smtp  
  permit tcp any any eq pop3  
ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf  
  permit udp any any range 16384 32767  
  permit tcp any any range 50000 59999  
ip access-list extended AutoQos-4.0-wlan-Acl-Scavanger  
  permit tcp any any range 2300 2400  
  permit udp any any range 2300 2400  
  permit tcp any any range 6881 6999  
  permit tcp any any range 28800 29100  
  permit tcp any any eq 1214  
  permit udp any any eq 1214  
  permit tcp any any eq 3689  
  permit udp any any eq 3689  
  permit tcp any any eq 11999  
ip access-list extended AutoQos-4.0-wlan-Acl-Signaling  
  permit tcp any any range 2000 2002  
  permit tcp any any range 5060 5061
```

```

permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data
permit tcp any any eq 443
permit tcp any any eq 1521
permit udp any any eq 1521
permit tcp any any eq 1526
permit udp any any eq 1526
permit tcp any any eq 1575
permit udp any any eq 1575
permit tcp any any eq 1630
permit udp any any eq 1630
permit tcp any any eq 1527
permit tcp any any eq 6200
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080
!
!
!
ipv6 access-list preauth_ipv6_acl
permit udp any any eq domain
permit tcp any any eq domain
permit icmp any any nd-ns
permit icmp any any nd-na
permit icmp any any router-solicitation
permit icmp any any router-advertisement
permit icmp any any redirect
permit udp any eq 547 any eq 546
permit udp any eq 546 any eq 547
deny ipv6 any any
!
control-plane
service-policy input system-cpp-policy
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
line vty 5 15
login
!
!
mac address-table notification mac-move
!
!
!
!
end

```

```
-----show switch | Include Ready-----
```

```
*1      Active   188b.9dfc.eb00    1      V00      Ready
```

```
----- show ipv6 mld snooping address | i FF02::5:1 -----
```

Vlan	Group	Type	Version	Port List
123	FF02::5:1	mld	v2	Gi2/0/1

show tech-support platform mld_snooping

Device#

出力フィールドの意味は自明です。

Related Commands

コマンド	説明
ipv6 mld snooping	MLDv2プロトコルスヌーピングをグローバルに有効にします。
show ipv6 mld snooping	MLDv2スヌーピング情報を表示します。
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support port

テクニカルサポートに使用するポート関連の情報を表示するには、特権 EXEC モードで **show tech-support port** コマンドを使用します。

show tech-support port

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Modes

特権 EXEC (#)

Command History

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

Usage Guidelines

show tech-support port コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support port | redirect flash:filename**）。

このコマンドの出力には次のコマンドが表示されます。

- **show clock**
- **show version**
- **show module**
- **show inventory**
- **show interface status**
- **show interface counters**
- **show interface counters errors**
- **show interfaces**
- **show interfaces capabilities**
- **show controllers**
- **show controllers utilization**
- **show idprom interface**
- **show controller ethernet-controller phy detail**
- **show switch**
- **show platform software fed switch active port summary**
- **show platform software fed switch ifm interfaces ethernet**
- **show platform software fed switch ifm mappings**

- show platform software fed switch ifm mappings lpn
- show platform software fed switch ifm mappings gpn
- show platform software fed switch ifm mappings port-le
- show platform software fed switch ifm if-id
- show platform software fed switch active port if_id

Examples

次に、**show tech-support port** コマンドの出力例を示します。

```
Device# show tech-support port
.
.
.
----- show controllers utilization -----

Port          Receive Utilization  Transmit Utilization
Gi1/0/1        0 0
Gi1/0/2        0 0
Gi1/0/3        0 0
Gi1/0/4        0 0
Gi1/0/5        0 0
Gi1/0/6        0 0
Gi1/0/7        0 0
Gi1/0/8        0 0
Gi1/0/9        0 0
Gi1/0/10       0 0
Gi1/0/11       0 0
Gi1/0/12       0 0
Gi1/0/13       0 0
Gi1/0/14       0 0
Gi1/0/15       0 0
Gi1/0/16       0 0
Gi1/0/17       0 0
Gi1/0/18       0 0
Gi1/0/19       0 0
Gi1/0/20       0 0
Gi1/0/21       0 0
Gi1/0/22       0 0
Gi1/0/23       0 0
Gi1/0/24       0 0
Gi1/0/25       0 0
Gi1/0/26       0 0
Gi1/0/27       0 0
Gi1/0/28       0 0
Gi1/0/29       0 0
Gi1/0/30       0 0
Gi1/0/31       0 0
Gi1/0/32       0 0
Gi1/0/33       0 0
Gi1/0/34       0 0
Gi1/0/35       0 0
Gi1/0/36       0 0
Te1/0/37       0 0
Te1/0/38       0 0
Te1/0/39       0 0
Te1/0/40       0 0
Te1/0/41       0 0
Te1/0/42       0 0
```

```
Tel/0/43      0  0
Tel/0/44      0  0
Tel/0/45      0  0
Tel/0/46      0  0
Tel/0/47      0  0
Tel/0/48      0  0
Tel/1/1       0  0
Tel/1/2       0  0
Tel/1/3       0  0
Tel/1/4       0  0
```

```
Total Ports : 52
Total Ports Receive Bandwidth Percentage Utilization : 0
Total Ports Transmit Bandwidth Percentage Utilization : 0
```

```
Average Switch Percentage Utilization : 0
```

```
----- show idprom interface Gi1/0/1 -----
```

```
*Sep  7 08:57:24.249: No module is present
```

```
.
.
.
```

出力フィールドの意味は自明です。

show tech-support pvlan

プライベート VLAN に関する情報を表示するには、特権 EXEC モードで **show tech-support pvlan** コマンドを使用します。

show tech-support pvlan [**pvlan_id** *pvlan-id*]

Syntax Description	pvlan_id <i>pvlan-id</i>	プライベート VLAN ID を指定します。
Command Default	特権 EXEC (#)	
Command History	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。
Usage Guidelines	<p>show tech-support pvlan コマンドの出力は非常に長くなります。この出力を効率よく処理するには、show tech-support pvlan [pvlan_id <i>vlan-id</i>] redirect location:filename を使用してローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。</p> <p>リダイレクトされたファイルの出力を表示するには、more location:filename コマンドを使用します。</p>	

show version

現在ロードされているソフトウェアの情報とハードウェアおよびデバイス情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show version** コマンドを使用します。

show version [**switch** ノード][**installed** | **provisioned** | **running**]

Syntax Description	switch ノード	(任意) 1つのスイッチのみを指定できます。デフォルトは、スタック構成のシステム内のすべてのスイッチです。
	running	(任意) 現在実行されているファイルに関する情報を指定します。
	provisioned	(任意) プロビジョニングされているソフトウェアファイルに関する情報を指定します。
	installed	RP にインストールされているソフトウェアに関する情報を指定します。
	user-interface	ユーザインターフェイスに関連するファイルに関する情報を指定します。

Command Default デフォルトの動作や値はありません。

Command Modes ユーザ EXEC (>)
特権 EXEC (#)

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドでは、デバイスで現在実行中の Cisco IOS ソフトウェアのバージョン、ROM モニタとブートフラッシュソフトウェアのバージョン、およびシステムメモリの量を含むハードウェア構成についての情報が表示されます。このコマンドではソフトウェアとハードウェアの両方の情報が表示されるため、このコマンドの出力は **show hardware** コマンドの出力と同じです (**show hardware** コマンドは **show version** コマンドのコマンドエイリアスです)。

show version コマンドは、具体的には次の情報を提供します。

- ソフトウェア情報
 - メインの Cisco IOS イメージのバージョン
 - メインの Cisco IOS イメージの機能 (フィーチャセット)
 - ROM 内のブートファイルの場所と名前
 - ブートフラッシュイメージのバージョン (プラットフォームによって異なる)
- デバイス固有の情報
 - デバイス名

- システムの動作期間
- システムのリロードの理由
- **config-register** 設定
- 次回のリロード後の **config-register** 設定（プラットフォームによって異なる）
- ハードウェア情報
 - プラットフォームタイプ
 - プロセッサ タイプ
 - プロセッサ ハードウェア リビジョン
 - 搭載されているメイン（プロセッサ）メモリの容量
 - 搭載されている I/O メモリの容量
 - 搭載されている各タイプのフラッシュメモリの容量（プラットフォームによって異なる）
 - プロセッサボード ID

このコマンドの出力の形式は次のとおりです。

```
Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>,
<software-type>

Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>

ROM: System Bootstrap, Version <software-version>, <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>, <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours,
<m> minutes
System returned to ROM by reload at <time> <day> <date>
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>Cisco <platform-processor-type>
processor (revision <processor-revision-id>) with <free-DRAM-memory>
K/<packet-memory>K bytes of memory.
Processor board ID <ID-number>

<CPU-type> CPU at <clock-speed>Mhz, Implementation <number>, Rev <
Revision-number>, <kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache
```

この出力のフィールドの説明については、「例」を参照してください。

show version を入力すると、IOS XE ソフトウェアのバージョンと IOS XE ソフトウェアバンドルが表示されます。このバンドルには、スイッチで実行されるソフトウェアの完全なセットを構成する一連の個別パッケージが含まれています。

show version running コマンドは、スイッチで現在実行されている個々のパッケージのリストを表示します。インストールモードで起動した場合、通常は起動したプロビジョニングファイルにリストされているパッケージのセットになります。バンドルモードで起動した場合、通常はバンドルに含まれているパッケージのセットになります。

show version provisioned コマンドは、プロビジョニングされたパッケージセットに関する情報を表示します。

次に、Cisco Catalyst 9300 シリーズ スイッチでの **show version** コマンドの出力例を示します。

```
Device# show version
Cisco IOS XE Software, Version BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Experimental Version
 16.10.20180903:072347
[v1610_throttle-/nobackup/mcpre/BLD-BLD_V1610_THROTTLE_LATEST_20180903_070602 183]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 03-Sep-18 11:53 by mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)
```

```
C9300 uptime is 20 hours, 7 minutes
Uptime for this control processor is 20 hours, 8 minutes
System returned to ROM by Image Install
System image file is "flash:packages.conf"
Last reload reason: Image Install
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

```
If you require further assistance please contact us by sending email to
export@cisco.com.
```

Technology Package License Information:

```
-----
Technology-package          Type          Technology-package
Current                    Next reboot
-----
network-advantage         Smart License    network-advantage
dna-advantage             Subscription Smart License    dna-advantage
```

```

Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco C9300-24U (X86) processor with 1415813K/6147K bytes of memory.
Processor board ID FCW2125L0BH
8 Virtual Ethernet interfaces
56 Gigabit Ethernet interfaces
16 Ten Gigabit Ethernet interfaces
4 TwentyFive Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
1638400K bytes of Crash Files at crashinfo-2:.
11264000K bytes of Flash at flash:.
11264000K bytes of Flash at flash-2:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address      : 70:d3:79:be:6c:80
Motherboard Assembly Number    : 73-17954-06
Motherboard Serial Number      : FOC21230KPX
Model Revision Number          : A0
Motherboard Revision Number    : A0
Model Number                   : C9300-24U
System Serial Number           : FCW2125L0BH

Switch Ports Model          SW Version  SW Image        Mode
-----
*   1 40   C9300-24U    16.10.1     CAT9K_IOSXE    INSTALL
   2 40   C9300-24U    16.10.1     CAT9K_IOSXE    INSTALL

Switch 02
-----
Switch uptime                : 20 hours, 8 minutes

Base Ethernet MAC Address    : 70:d3:79:84:85:80
Motherboard Assembly Number  : 73-17954-06
Motherboard Serial Number    : FOC21230KPK
Model Revision Number        : A0
Motherboard Revision Number  : A0
Model Number                 : C9300-24U
System Serial Number         : FCW2125L03W
Last reload reason           : Image Install

```

Configuration register is 0x102

次に、Cisco Catalyst 9300 シリーズスイッチで **show version running** コマンドを入力して、2メンバスタックの両方のスイッチで現在実行されているパッケージに関する情報を表示する例を示します。

```

Device# show version running
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
  Role: rp_base

```

```
File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
Role: rp_boot
File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: n/a

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
Role: guestshell
File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
Role: rp_daemons
File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
Role: rp_iosd
File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
Role: rp_security
File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
Role: rp_webui
File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
Role: srdriver
File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
```

```

status: active
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7

```

次に、2 メンバスタックのアクティブスイッチである Cisco Catalyst 9300 シリーズ スイッチで **show version provisioned** コマンドを入力した場合の例を示します。 **show version provisioned** コマンドは、プロビジョニングされたパッケージセットに含まれているパッケージに関する情報を表示します。

```

Device# show version provisioned
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_base
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: guestshell
  File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_boot
  File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: n/a

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_daemons
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_iosd
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:

```

```
n/a
  Role: rp_security
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
  on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_webui
  File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
  on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: wlc, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_wlc
  File: /flash/cat9k-wlc.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
  on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: ada21bb3d57e1b03e5af2329503ed6caa7236d6e

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: srdriver
  File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: espbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: fp
  File: /flash/cat9k-espbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
  on: ESP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 1a2317485f285a3945b31ae57aa64c56ed30a8c0

Package: sipbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: cc
  File: /flash/cat9k-sipbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
  on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: ce821195f0c0bd5e44f21e32fca76cf9b2eed02b

Package: sipspa, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: cc_spa
  File: /flash/cat9k-sipspa.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
  on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 54645404860b662d72f8ff7fa5e6e88cb0960e20

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
  on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7
```

Table 167: 表 5, *show version running* のフィールドの説明

フィールド	説明
Package:	個々のサブパッケージの名前。
version:	個々のサブパッケージのバージョン。
status:	特定のスーパーバイザモジュールに対してパッケージがアクティブであるか非アクティブであるか。
File:	個々のパッケージファイルのファイル名。
on:	このパッケージが実行されているアクティブまたはスタンバイのスーパーバイザのスロット番号。
Built:	個々のパッケージが作成された日付。

system env temperature threshold yellow

イエローのしきい値を決定する、イエローとレッドの温度しきい値の差を設定するには、グローバルコンフィギュレーションコマンドで **system env temperature threshold yellow** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system env temperature threshold yellow *value*
no system env temperature threshold yellow *value*

Syntax Description

value イエローとレッドのしきい値の差を指定します（摂氏）。指定できる範囲は10～25です。

Command Default

デフォルト値は次のとおりです。

Table 168: 温度しきい値のデフォルト値

デバイス	イエローとレッドの差	レッド ¹⁰
	14 °C	60 °C

¹⁰ レッドの温度しきい値を設定することはできません。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

グリーンとレッドのしきい値を設定することはできませんが、イエローのしきい値を設定することはできます。イエローとレッドのしきい値の差を指定して、イエローのしきい値を設定するには、**system env temperature threshold yellow** *value* グローバルコンフィギュレーションコマンドを使用します。たとえば、レッドしきい値が66°Cの場合に、イエローしきい値を51°Cに設定するには、しきい値の差を15に設定するために、**system env temperature threshold yellow 15** コマンドを使用します。たとえば、レッドしきい値が60°Cの場合に、イエローしきい値を51°Cに設定するには、しきい値の差を15に設定するために、**system env temperature threshold yellow 9** コマンドを使用します。



Note デバイス内部の温度センサーでシステム内の温度を測定するため、±5°Cの差が生じる可能性があります。

Examples

次の例では、イエローとレッドのしきい値の差を15に設定する方法を示します。

system env temperature threshold yellow

```
Device(config)# system env temperature threshold yellow 15  
Device(config)#
```

tftp-server

ルータまたはルータ上のフラッシュメモリデバイスを TFTP サーバーとして設定するには、グローバルコンフィギュレーションモードで次の **tftp-server** コマンドを使用します。前に定義したファイル名を削除するには、このコマンドの **no** 形式に適切なファイル名を指定して使用します。

```
tftp-server [ bootflash | crashinfo | disk0 | flash | null | nvram | rom | system | tmpsys ] { <1-99> | <1300-1999> | alias }
```

```
no tftp-server [ bootflash | crashinfo | disk0 | flash | null | nvram | rom | system | tmpsys ] { <1-99> | <1300-1999> | alias }
```

Command Default

デフォルトの動作や値はありません。

Syntax Description

bootflash	フラッシュメモリデバイス上のファイルの TFTP サービスを指定します。
crashinfo	ブートフラッシュまたはフラッシュメモリに保存されている、最新のクラッシュに関する有用な情報を集めたもの。
disk0	ローテーションメディアの送信元または宛先 URL。
flash	フラッシュメモリ内のファイルの TFTP サービスを指定します。
null	ヌルのコピー先またはファイル。リモートファイルをヌルにコピーすると、サイズを確認できます。
nvram	デバイスの NVRAM。
rom	ROM 内のファイルの TFTP サービスを指定します。
system	実行コンフィギュレーションを含む、システムメモリの送信元または宛先 URL。

alias

TFTP サーバーが TFTP 読み取り要求に応答する際に使用するファイルの代替名を指定します。

Usage Guidelines

tftp-server コマンドを繰り返すことによって、複数のファイル名を指定できます。システムは、ROMに含まれるシステムイメージのコピー、またはフラッシュメモリに含まれるシステムイメージの1つを、このファイル名を使用して TFTP 読み取り要求を発行するすべてのクライアントに送信します。

指定した *filename1* または *filename2* 引数がフラッシュメモリに存在する場合は、フラッシュイメージのコピーが送信されます。ROM に完全なイメージが含まれているシステムでは、指定された *filename1* または *filename2* 引数がフラッシュメモリにない場合、ROM イメージが送信されます。

ROMから実行されるイメージをネットワーク経由でロードすることはできません。したがって、TFTP を使用してこれらのイメージの ROM を提供しても意味がありません。

USB が TFTP サーバーとして設定されている場合は、USB を物理的に取り外すか無効にする前に、対応するすべての設定を削除することをお勧めします。USB が無効になるか、または物理的に取り外されると、USB オプションは使用できなくなります。

Command Modes

グローバル設定

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

次に、デバイスが TFTP サーバーとして動作できるようにする例を示します。ソースファイル *c3640-i-mz* は、内部フラッシュメモリの 2 番目のパーティションにあります。

```
Device (config)# tftp-server flash flash:2:dirt/gate/c3640-i-mz
```

traceroute mac

指定の送信元 MAC アドレスから指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac** コマンドを使用します。

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*]
destination-mac-address [**vlan** *vlan-id*] [**detail**]

Syntax Description	
interface <i>interface-id</i>	(任意) 送信元または宛先デバイス上のインターフェイスを指定します。
<i>source-mac-address</i>	送信元デバイスの 16 進形式の MAC アドレス。
<i>destination-mac-address</i>	宛先デバイスの 16 進形式の MAC アドレス。
vlan <i>vlan-id</i>	(任意) 送信元デバイスから宛先デバイスまでをパケットが通過するレイヤ 2 のパスをトレースする VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 4094 です。
detail	(任意) 詳細情報を表示するよう指定します。

Command Default デフォルトの動作や値はありません。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines レイヤ 2 のトレースルートを適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークのすべてのデバイスでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

デバイスがレイヤ 2 パス内でレイヤ 2 トレースルートをサポートしていないデバイスを検知した場合、デバイスはレイヤ 2 トレースクエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 10 です。

レイヤ 2 **traceroute** はユニキャストトラフィックだけをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、エラーメッセージが表示されます。

指定された送信元および宛先アドレスが同じ VLAN にある場合、**traceroute mac** コマンド出力はレイヤ 2 パスを表示します。

異なる VLAN にある送信元および宛先アドレスを指定した場合、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。

送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。

VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを介して1つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 **tracert** 機能はサポートされません。

複数の CDP ネイバーが1つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5       ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1       ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2       ) :   Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
      Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先デバイスのインターフェイスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5       ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1       ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2       ) :   Gi0/0/2 => Gi0/0/1
```

```
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、デバイスが送信元デバイスに接続されていない場合のレイヤ2のパスを示します。

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
con5 / WS-C3750E-24TD / 2.2.5.5 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、デバイスが送信元MACアドレスの宛先ポートを検出できない場合のレイヤ2のパスを示します。

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ2のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

次の例では、宛先MACアドレスがマルチキャストアドレスの場合のレイヤ2のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

次の例では、送信元および宛先デバイスが複数の VLAN にある場合のレイヤ2のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

tracroute mac ip

指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示するには、特権 EXEC モードで **tracroute mac ip** コマンドを使用します。

tracroute mac ip {*source-ip-address source-hostname*} {*destination-ip-address destination-hostname*}
[**detail**]

Syntax Description	
<i>source-ip-address</i>	32 ビットの値（ドット付き 10 進表記）で指定された送信元デバイスの IP アドレス。
<i>source-hostname</i>	送信元デバイスの IP ホスト名。
<i>destination-ip-address</i>	32 ビットの値（ドット付き 10 進表記）で指定された宛先デバイスの IP アドレス。
<i>destination-hostname</i>	宛先デバイスの IP ホスト名。
detail	（任意）詳細情報を表示するよう指定します。

Command Default デフォルトの動作や値はありません。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines レイヤ 2 のトレースルートを適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークの各デバイスでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

デバイスがレイヤ 2 パス内でレイヤ 2 トレースルートをサポートしていないデバイスを検知した場合、デバイスはレイヤ 2 トレースクエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 10 です。

指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**tracroute mac ip** コマンド出力はレイヤ 2 パスを表示します。

IP アドレスを指定した場合、デバイスは Address Resolution Protocol (ARP) を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を対応させます。

- 指定の IP アドレスの ARP のエントリが存在している場合、デバイスは関連付けられた MAC アドレスを使用し、物理パスを識別します。

- ARP のエントリが存在しない場合、デバイスは ARP クエリを送信し、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されない場合は、パスは識別されず、エラーメッセージが表示されます。

複数の装置がハブを介して1つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。

複数の CDP ネイバーが1つのポートで検出された場合、レイヤ 2 パスは特定されず、エラーメッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、**detail** キーワードを使用して、送信元と宛先の IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5)   ) :   Gi0/0/3 => Gi0/1
con1          (2.2.1.1)   ) :   Gi0/0/1 => Gi0/2
con2          (2.2.2.2)   ) :   Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
Device# tracert mac ip 2.2.66.66 2.2.77.77  
Arp failed for destination 2.2.77.77.  
Layer2 trace aborted.
```

type

1 つ以上のファイルの内容を表示するには、ブートローダモードで **type** コマンドを使用します。

type *filesystem:/file-url...*

Syntax Description

filesystem: ファイルシステムのエイリアス。システム ボードフラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。

/file-url... 表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ファイルのリストを指定すると、各ファイルの内容が順次表示されます。

Examples

次に、ファイルの内容を表示する例を示します。

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

1つ以上の環境変数をリセットするには、ブートローダモードで **unset** コマンドを使用します。

unset variable...

Syntax Description

variable

variable には、次に示すキーワードのいずれかを使用します。

MANUAL_BOOT/MANUAL_BOOT: デバイスの起動を自動で行うか手動で行うかどうかを指定します。

BOOT: 自動起動時に、実行可能ファイルのリストをリセットして、ロードおよび実行します。**BOOT** 環境変数が設定されていない場合、システムは、フラッシュファイルシステム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。**BOOT** 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュファイルシステムで最初に検出した起動可能なファイルを起動しようとします。

ENABLE_BREAK: フラッシュファイルシステムの初期化後に、コンソール上の **Break** キーを使用して自動ブートプロセスを中断できるかどうかを指定します。

HELPER: ブートローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパーファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。

PS1: ブートローダモードの場合に、コマンドラインプロンプトとして使用する文字列を指定します。

CONFIG_FILE: Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名をリセットします。

BAUD: コンソールで使用される速度（ビット/秒（b/s）単位）をリセットします。コンフィギュレーションファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボーレート設定を継承し、この値を引き続き使用します。

Command Default

デフォルトの動作や値はありません。

Command Modes

ブートローダ

Command History

リリース

変更内容

Cisco IOS XE Fuji
16.9.2

このコマンドが導入されました。

Usage Guidelines

通常的环境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**no boot manual** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

BOOT 環境変数は、**no boot system** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

ENABLE_BREAK 環境変数は、**no boot enable-break** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

HELPER 環境変数は、**no boot helper** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

CONFIG_FILE 環境変数は、**no boot config-file** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

例

次に、SWITCH_PRIORITY 環境変数をリセットする例を示します。

```
Device: unset SWITCH_PRIORITY
```

version

ブートローダのバージョンを表示するには、ブートローダモードで **version** コマンドを使用します。

version [-v]

Syntax Description	▼ ハードウェアアンカー、マイクロローダ、ファームウェア DDR および ROMMON リビジョンのバージョンを表示します。				
Command Default	デフォルトの動作や値はありません。				
Command Modes	ブートローダ				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Examples

次に、デバイスのブートローダのバージョンを表示する例を示します。

```
Device: version -v
System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)
Compiled Tue 09/04/2018 22:58:10 by rel

Current ROMMON image : Primary
C9200-48P-4X platform with 2097152 Kbytes of main memory

HARDWARE ANCHOR : v027.0  crayprod_20160517 20160517-2135
MICROLOADER      : v061.0  rel_16_10_1r 20180904-2252
FIRMWARE-DDR    : v011.0  rel_16_10_1r 20180904-2254
ROMMON REVISION : v010.003
```



トレース

- [トレースについて](#), on page 1942
- [set platform software trace](#), on page 1945
- [show platform software trace filter-binary](#), on page 1949
- [show platform software trace message](#), on page 1950
- [show platform software trace level](#), on page 1954
- [request platform software trace archive](#), on page 1958
- [request platform software trace rotate all](#), on page 1959
- [request platform software trace filter-binary](#), on page 1960

トレースについて

トレースの概要

トレース機能により内部イベントが記録されます。トレースファイルは自動的に作成され、`crashinfo` の下の `tracelogs` サブディレクトリに保存されます。

トレースファイルのデータは、次の処理を行う場合に役立ちます。

- **トラブルシューティング**: スイッチに問題がある場合、トレースファイルの出力により、問題の特定および解決に使用できる情報が得られる場合があります。
- **デバッグ**: トレースファイルの出力は、システム動作の詳細情報を得るために役立ちます。

特定のモジュールに関する最新のトレース情報を表示するには、**`show platform software trace message`** コマンドを使用します。

トレースレベルを変更してトレースメッセージ出力の量を調整するために、**`set platform software trace`** コマンドを使用して新しいトレーシングレベルを設定できます。トレースレベルは、**`set platform software trace`** コマンドで **`all-modules`** キーワードを使用してプロセスごとに設定することも、プロセス内のモジュールごとに設定することもできます。

トレースログの場所

各プロセスは、`btrace` インフラストラクチャを使用してトレースメッセージをログに記録します。プロセスがアクティブのときは、対応するインメモリトレースログが `/tmp/<FRU>/trace/` ディレクトリにあります。ここで、`<FRU>` は、プロセスが実行されている場所 (`rp`、`fp`、または `cc`) を表します。

トレースログファイルがプロセスに関して許可されている最大ファイルサイズの上限に達すると、またはプロセスが終了すると、次のディレクトリにローテーションされます。

- `/crashinfo/tracelogs` (スイッチで `crashinfo`: パーティションを使用できる場合)
- `/harddisk/tracelogs` (スイッチで `crashinfo`: パーティションを使用できない場合)

トレースログファイルは、ディレクトリに保存される前に圧縮されます。

トレースログの命名規則

`btrace` を使用して作成されるすべてのトレースログには、次の命名規則が適用されます。

`<process_name>_<FRU><SLOT>-<BAY>.<pid>_<counter>.<creation_timestamp>.bin`

ここで、`counter` は、64 ビットのフリーランニングカウンタで、当該プロセスの新しいファイルが作成されるたび増加します。たとえば、`wcm_R0-0.1362_0.20151006171744.bin` ようになります。圧縮されると、ファイル名に `gz` 拡張子が付加されます。

トレースログのサイズの上限およびローテーションポリシー

トレースログファイルの最大サイズはプロセスごとに 1 MB で、保持されるトレースログファイルの最大数はプロセスごとに 25 です。

ローテーションおよびスロットリングポリシー

最初は、すべてのトレースログファイルが、初期ディレクトリの /tmp/<FRU>/trace から中継ディレクトリの /tmp/<FRU>/trace/stage に移されます。次に、btrace_rotate スクリプトによって、これらのトレースログが中継ディレクトリから /crashinfo/tracelogs ディレクトリに移されます。プロセスごとに /crashinfo/tracelogs ディレクトリに保存されるファイルの数が最大数の上限に達すると、そのプロセスの最も古いファイルが削除されますが、それより新しいファイルは保持されます。これは、最悪の場合、60 分ごとに繰り返されます。

その他、次の 2 種類のファイルセットが /crashinfo/tracelogs ディレクトリからパージされます。

- 標準命名規則を持たないファイル (fed_python.log などのいくつかの例外を除く)
- 2 週間以上保持されたファイル

エラーのあるプロセスがスイッチの機能に影響を与えないように、スロットリングポリシーが導入されました。プロセスが非常に高い頻度でログを記録する（たとえば、そのプロセスに関して中継ディレクトリに 4 秒間隔で 17 以上のファイルが保存される）場合は常に、そのプロセスがスロットリングされます。そのプロセスのファイルは /tmp/<FRU>/trace から /tmp/<FRU>/trace/stage にローテーションされませんが、最大サイズに達すると削除されます。ファイル数が 7 以下になるとスロットリングが再度有効になります。

トレースレベル

トレースレベルは、トレースバッファまたはトレースファイルに保存する必要のあるモジュール情報の量を決定します。

次の表に、使用可能なすべてのトレースレベルを示し、各トレースレベルで表示されるメッセージについて説明します。

表 169: トレースレベルとその内容

トレースレベル	説明
緊急	システムが使用不能になる問題のメッセージです。
Error	システムエラーについてのメッセージです。
警告	システム警告についてのメッセージです。
Notice	重大な問題に関するメッセージです。ただし、スイッチは通常どおり動作しています。

トレースレベル	説明
Informational	単に情報を提供するだけのメッセージです。
デバッグ	デバッグレベルの出力を提供するメッセージです。
詳細	生成可能なすべてのトレースメッセージが送信されます。
Noise	モジュールについての生成可能なすべてのトレースメッセージが記録されます。 ノイズレベルは常に最上位のトレースレベルに相当します。今後、トレース機能の拡張が行われ、さらに低いトレースレベルが導入された場合でも、ノイズレベルはこの新しい拡張機能のレベルと同じレベルに相当します。

set platform software trace

プロセス内の特定のモジュールのトレースレベルを設定するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software trace** コマンドを使用します。

set platform software trace *process slot module trace-level*

Syntax Description

process

トレースレベルが設定されているプロセス。次のオプションがあります。

- **chassis-manager**: Chassis Manager プロセス。
 - **cli-agent**: CLI Agent プロセス。
 - **dbm**: Database Manager プロセス。
 - **emd**: Environmental Monitoring プロセス。
 - **fed**: Forwarding Engine Driver プロセス。
 - **forwarding-manager**: Forwarding Manager プロセス。
 - **host-manager**: Host Manager プロセス。
 - **iomd**: Input/Output Module daemon (IOMd) プロセス。
 - **ios**: IOS プロセス。
 - **license-manager**: License Manager プロセス。
 - **logger**: Logging Manager プロセス。
 - **platform-mgr**: Platform Manager プロセス。
 - **pluggable-services**: Pluggable Services プロセス。
 - **replication-mgr**: Replication Manager プロセス。
 - **shell-manager**: Shell Manager プロセス。
 - **smd**: Session Manager プロセス。
 - **table-manager**: Table Manager サーバ。
 - **wireshark**: Embedded Packet Capture (EPC) Wireshark プロセス。
-

<i>slot</i>	<p>トレースレベルが設定されているプロセスを実行中のハードウェアスロット。次のオプションがあります。</p> <ul style="list-style-type: none">• number: トレースレベルが設定されているハードウェアモジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。• SIP-slot/SPA-bay: SIP スイッチスロットの数とその SIP の共有ポートアダプタ (SPA) ベイの数。たとえば、スイッチスロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。• F0: スロット 0 の Embedded-Service-Processor。• FP active: アクティブな Embedded-Service-Processor。• R0: スロット 0 のルートプロセッサ。• RP active: アクティブなルートプロセッサ。• switch <number> : 指定された番号を持つスイッチ。• switch active: アクティブなスイッチ。• switch standby: スタンバイスイッチ。
<i>module</i>	<p>トレースレベルが設定されているプロセス内のモジュール。</p>

trace-level

トレース レベルです。次のオプションがあります。

- **debug:** デバッグ レベルのトレーシング。デバッグレベルのトレースメッセージは、モジュールに関する大量の詳細を提供する緊急でないメッセージです。
- **emergency:** 緊急事態レベルのトレーシング。緊急レベルのトレースメッセージは、システムが使用不能であることを示すメッセージです。
- **error:** エラー レベルのトレーシング。エラーレベルのトレースメッセージは、システム エラーを示すメッセージです。
- **info:** 情報レベルのトレーシング。情報レベルのトレースメッセージは、システムに関する情報を提供する緊急でないメッセージです。
- **noise:** ノイズ レベルのトレーシング。ノイズレベルは、常に可能なトレースレベルの中の最高レベルに相当し、考えられるすべてのトレースメッセージを生成します。

ノイズレベルは、モジュールに関して可能な最高レベルのトレースメッセージに相当します。これは、このコマンドの将来の拡張で、ユーザが寄り高いトレースレベルを設定できるオプションが追加された場合にも、当てはまります。

- **notice:** 重大な問題に関するメッセージです。ただし、スイッチは通常どおり動作しています。
- **verbose:** 詳細レベルのトレーシング。トレースレベルが **verbose** に設定されている場合は、考えられるすべてのトレースメッセージが送信されます。
- **warning:** 警告メッセージ。

Command Default

すべてのモジュールのデフォルトのトレースレベルは **notice** です。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース	変更内容
------	------

このコマンドが導入されました。

Usage Guidelines

module オプションは、プロセスおよび *hardware-module* によって異なります。このコマンドを入力する際に、各キーワードシーケンスで使用可能な *module* オプションを確認するには、? オプションを使用します。

トレースメッセージを表示するには、**show platform software trace message** コマンドを使用します。

トレースファイルは、**harddisk:** ファイルシステムのトレースログディレクトリに保存されます。これらのファイルは、スイッチの動作に影響を与えずに削除できます。

トレースファイル出力は、デバッグに使用されます。トレースレベルは、モジュールに関するどのぐらいの量の情報をトレースファイルに保存するかを決定する設定です。

Examples

次に、dbm プロセスのすべてのモジュールのトレース レベルを設定する例を示します。

```
デバイス# set platform software trace dbm R0 all-modules debug
```

show platform software trace filter-binary

特定のモジュールの最新のトレース情報を表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show platform software trace filter-binary** コマンドを使用します。

show platform software trace filter-binary *modules* [**context** *mac-address*]

Syntax Description

context*mac-address*

フィルタ処理に使用されるコンテキストを表します。また、モジュール名とトレースレベルに基づいてフィルタ処理できます。コンテキストキーワードは、タグが付いているトレースに基づき MAC アドレスまたは他の引数を受け入れます。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース 変更内容
ス

このコマンドが導入されました。

Usage Guidelines

このコマンドは、モジュールに関連するすべてのプロセス全体で /tmp/.../ に存在するすべてのログを照合してソートします。指定されたモジュールに関連するすべてのプロセスのトレースログがコンソールに出力されます。このコマンドでは、同じコンテンツの `collated_log_{system time}` という名前のファイルも /crashinfo/tracelogs ディレクトリに生成されます。

show platform software trace message

プロセスのトレースメッセージを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software trace** コマンドを使用します。

show platform software trace message *process slot*

Syntax Description*process*

設定されているトレースレベル。次のオプションがあります。

- **chassis-manager**: Chassis Manager プロセス。
- **cli-agent**: CLI Agent プロセス。
- **cmm**: CMM プロセス。
- **dbm**: Database Manager プロセス。
- **emd**: Environmental Monitoring プロセス。
- **fed**: Forwarding Engine Driver プロセス。
- **forwarding-manager**: Forwarding Manager プロセス。
- **geo**: Geo Manager プロセス。
- **host-manager**: Host Manager プロセス。
- **interface-manager**: Interface Manager プロセス。
- **iomd**: Input/Output Module daemon (IOMd) プロセス。
- **ios**: IOS プロセス。
- **license-manager**: License Manager プロセス。
- **logger**: Logging Manager プロセス。
- **platform-mgr**: Platform Manager プロセス。
- **pluggable-services**: Pluggable Services プロセス。
- **replication-mgr**: Replication Manager プロセス。
- **shell-manager**: Shell Manager プロセス。
- **sif**: Stack Interface (SIF) Manager プロセス。
- **smd**: Session Manager プロセス。
- **stack-mgr**: Stack Manager プロセス。
- **table-manager**: Table Manager サーバ。
- **thread-test**: Multithread Manager プロセス。
- **virt-manager**: Virtualization Manager プロセス。

slot

トレースレベルが設定されているプロセスを実行中のハードウェアスロット。次のオプションがあります。

- **number:** トレースレベルが設定されているハードウェアモジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
 - **SIP-slot/SPA-bay:** SIP スイッチスロットの数とその SIP の共有ポートアダプタ (SPA) ベイの数。たとえば、スイッチスロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
 - **F0:** Embedded Service Processor スロット 0。
 - **FP active:** アクティブな Embedded Service Processor。
 - **R0:** スロット 0 のルートプロセッサ。
 - **RP active:** アクティブなルートプロセッサ。
 - **switch <number> :** 指定された番号を持つスイッチ。
 - **switch active:** アクティブなスイッチ。
 - **switch standby:** スタンバイスイッチ。
 - **number:** トレースレベルが設定されているハードウェアモジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
 - **SIP-slot/SPA-bay:** SIP スイッチスロットの数とその SIP の共有ポートアダプタ (SPA) ベイの数。たとえば、スイッチスロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
 - **F0:** スロット 0 の Embedded Service Processor。
 - **FP active:** アクティブな Embedded Service Processor。
 - **R0:** スロット 0 のルートプロセッサ。
 - **RP active:** アクティブなルートプロセッサ。
-

Command Modes ユーザ EXEC (>)

特権 EXEC (#)

Command History リリリー 変更内容
ス

 このコマンドが導入されました。

Examples

次に、Stack Manager プロセスおよび Forwarding Engine Driver プロセスのトレースメッセージを表示する例を示します。

```

デバイス# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

デバイス# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]: UUID: 0, ra: 0 (note): Single message size is greater
than 1024
11/02 10:55:01.822 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module
[88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module
[89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]: UUID: 0, ra: 0 (note): Pending connection to server
10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]: UUID: 0, ra: 0 (ERR): FRU hardware authentication Fail,
result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C receive
failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR):
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR):

```

show platform software trace level

特定のプロセスですべてのモジュールのトレース レベルを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show platform software trace level** コマンドを使用します。

show platform software trace level *process slot*

Syntax Description*process*

トレースレベルが設定されているプロセス。次のオプションがあります。

- **chassis-manager**: Chassis Manager プロセス。
- **cli-agent**: CLI Agent プロセス。
- **cmm**: CMM プロセス。
- **dbm**: Database Manager プロセス。
- **emd**: Environmental Monitoring プロセス。
- **fed**: Forwarding Engine Driver プロセス。
- **forwarding-manager**: Forwarding Manager プロセス。
- **geo**: Geo Manager プロセス。
- **host-manager**: Host Manager プロセス。
- **interface-manager**: Interface Manager プロセス。
- **iomd**: Input/Output Module daemon (IOMd) プロセス。
- **ios**: IOS プロセス。
- **license-manager**: License Manager プロセス。
- **logger**: Logging Manager プロセス。
- **platform-mgr**: Platform Manager プロセス。
- **pluggable-services**: Pluggable Services プロセス。
- **replication-mgr**: Replication Manager プロセス。
- **shell-manager**: Shell Manager プロセス。
- **sif**: Stack Interface (SIF) Manager プロセス。
- **smd**: Session Manager プロセス。
- **stack-mgr**: Stack Manager プロセス。
- **table-manager**: Table Manager サーバ。
- **thread-test**: Multithread Manager プロセス。
- **virt-manager**: Virtualization Manager プロセス。

slot トレースレベルが設定されているプロセスを実行中のハードウェア スロット。次のオプションがあります。

- **number:** トレースレベルが設定されているハードウェアモジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
- **SIP-slot/SPA-bay:** SIP スイッチ スロットの数とその SIP の共有ポートアダプタ (SPA) ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
- **F0:** スロット 0 の Embedded Service Processor。
- **F1:** スロット 1 の Embedded Service Processor。
- **FP active:** アクティブな Embedded Service Processor。
- **R0:** スロット 0 のルートプロセッサ。
- **RP active:** アクティブなルートプロセッサ。
- **switch <number>:** 指定された番号を持つスイッチ。
- **switch active:** アクティブなスイッチ。
- **switch standby:** スタンバイスイッチ。
 - **number:** トレースレベルが設定されているハードウェアモジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
 - **SIP-slot/SPA-bay:** SIP スイッチ スロットの数とその SIP の共有ポートアダプタ (SPA) ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
 - **F0:** スロット 0 の Embedded Service Processor。
 - **FP active:** アクティブな Embedded Service Processor。
 - **R0:** スロット 0 のルートプロセッサ。
 - **RP active:** アクティブなルートプロセッサ。

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース 変更内容
ス

このコマンドが導入されました。

Examples

次に、トレース レベルを表示する例を示します。

```

デバイス# show platform software trace level dbm switch active R0
Module Name                               Trace Level
-----
binos                                       Notice
binos/brand                                Notice
bipc                                        Notice
btrace                                      Notice
bump_ptr_alloc                             Notice
cdllib                                      Notice
chasfs                                      Notice
dbal                                        Informational
dbm                                         Debug
evlib                                       Notice
evutil                                      Notice
file_alloc                                 Notice
green-be                                    Notice
ios-avl                                     Notice
klib                                        Debug
services                                   Notice
sw_wdog                                    Notice
syshw                                       Notice
tdl_cdlcore_message                        Notice
tdl_dbal_root_message                      Notice
tdl_dbal_root_type                         Notice

```

request platform software trace archive

スイッチでの最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、これを指定された場所に保存するには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace archive** コマンドを使用します。

request platform software trace archive [*last number-of-days* [*days* [*target location*]] | *target location*]

Syntax Description

last <i>noofdays</i>	トレースファイルをアーカイブする必要がある日数を指定します。
target <i>location</i>	アーカイブ ファイルの場所と名前を指定します。

Command Modes

ユーザ EXEC (>)
特権 EXEC (#)

Command History

リリー 変更内容
ス

このコマンドが導入されました。

Usage Guidelines

このアーカイブ ファイルは、`tftp` コマンドまたは `scp` コマンドを使用してシステムからコピーできます。

Examples

次に、過去5日以降にスイッチで実行されているプロセスのすべてのトレースログをアーカイブする例を示します。

```
デバイス# request platform software trace archive last 5 days target flash:test_archive
```

request platform software trace rotate all

現在のインメモリトレースログを crashinfo パーティションに循環させ、プロセスごとの新しいインメモリトレースログを開始するには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace rotate all** コマンドを使用します。

request platform software trace rotate all

Command Modes

ユーザ EXEC (>)

特権 EXEC (#)

Command History

リリース 変更内容
ス

このコマンドが導入されました。

Usage Guidelines

トレースログファイルは読み取り専用を目的としています。ファイルの内容は編集しないでください。特定のログセットを表示するために、ファイルの内容を削除する必要がある場合は、このコマンドを使用して新しいトレース ログ ファイルを開始します。

Examples

次に、過去1日以降にスイッチで実行されているプロセスのすべてのインメモリトレースログを循環させる例を示します。

```
デバイス# request platform software trace slot switch active R0 archive last 1 days target flash:test
```

request platform software trace filter-binary

トレースログサブディレクトリに存在するすべてのアーカイブログを照合して並べ替えるには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace filter-binary** コマンドを使用します。

```
request platform software trace filter-binary modules [context mac-address]
```

Syntax Description	context <i>mac-address</i>	フィルタ処理に使用されるコンテキストを表します。また、モジュール名とトレースレベルに基づいてフィルタ処理できます。コンテキストキーワードは、タグが付いているトレースに基づき MAC アドレスまたは他の引数を受け入れます。
Command Modes	ユーザ EXEC (>) 特権 EXEC (#)	
Command History	リリース 変更内容 ス	このコマンドが導入されました。
Usage Guidelines	このコマンドは、モジュールに関連するすべてのプロセスを対象に、トレースログサブディレクトリに存在するすべてのアーカイブされたログを照合して並べ替えます。このコマンドでは、同じコンテンツの <code>collated_log_{system time}</code> という名前のファイルも <code>/crashinfo/tracelogs</code> ディレクトリに生成されます。	



PART XIII

VLAN

- [VLAN コマンド](#), on page 1963



VLAN コマンド

- [clear vtp counters](#), on page 1964
- [debug sw-vlan](#), on page 1965
- [debug sw-vlan ifs](#), on page 1967
- [debug sw-vlan notification](#), on page 1968
- [debug sw-vlan vtp](#), on page 1970
- [private-vlan](#), on page 1972
- [private-vlan mapping](#), on page 1975
- [show interfaces private-vlan mapping](#), on page 1977
- [show vlan](#), on page 1978
- [show vtp](#), on page 1982
- [switchport mode private-vlan](#), on page 1989
- [switchport priority extend](#), on page 1991
- [switchport trunk](#), on page 1992
- [vlan](#), on page 1995
- [vlan dot1q tag native](#), on page 2003
- [vtp \(グローバル コンフィギュレーション\)](#) , on page 2004
- [vtp \(インターフェイス コンフィギュレーション\)](#) , on page 2010
- [vtp primary](#), on page 2011

clear vtp counters

VLAN Trunking Protocol (VTP) およびプルーニングカウンタをクリアするには、特権 EXEC モードで **clear vtp counters** コマンドを使用します。

clear vtp counters

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Examples

次の例では、VTP カウンタをクリアする方法を示します。

```
Device> enable
Device# clear vtp counters
```

情報が削除されたことを確認するには、**show vtp counters** 特権 EXEC コマンドを入力します。

debug sw-vlan

VLAN マネージャアクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification | packets
| redundancy | registries | vtp}
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification | packets
| redundancy | registries | vtp}
```

Syntax Description

badpmcookies	不良ポートマネージャクッキーの VLAN マネージャインシデントに関するデバッグメッセージを表示します。
cfg-vlan	VLAN 設定デバッグメッセージを表示します。
bootup	スイッチが起動すると、メッセージが表示されます。
cli	コマンドライン インターフェイス (CLI) が VLAN コンフィギュレーション モードである場合のメッセージを表示します。
events	VLAN マネージャ イベントのデバッグメッセージを表示します。
ifs	VLAN マネージャ IOS ファイル システム (IFS) のデバッグメッセージを表示します。詳細については、「 debug sw-vlan ifs, on page 1967 」を参照してください。
mapping	VLAN マッピングのデバッグメッセージを表示します。
notification	VLAN マネージャ通知のデバッグメッセージを表示します。詳細については、「 debug sw-vlan notification, on page 1968 」を参照してください。
packets	パケット処理およびカプセル化プロセスのデバッグメッセージを表示します。
redundancy	VTP VLAN 冗長性のデバッグメッセージを表示します。
registries	VLAN マネージャ レジストリのデバッグメッセージを表示します。
vtp	VLAN Trunking Protocol (VTP) コードのデバッグメッセージを表示します。詳細については、「 debug sw-vlan vtp, on page 1970 」を参照してください。

Command Default

デバッグはディセーブルです。

Command Modes

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

undebg sw-vlan コマンドは **no debug sw-vlan** コマンドと同じです。

Examples

次に、VLAN マネージャ イベントのデバッグ メッセージを表示する例を示します。

```
Device> enable
Device# debug sw-vlan events
```

debug sw-vlan ifs

VLAN マネージャ IOS File System (IFS) エラーテストのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan ifs** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

Syntax Description	open read	VLAN マネージャ IFS ファイル読み取り動作のデバッグ メッセージを表示します。
	open write	VLAN マネージャ IFS ファイル書き込み動作のデバッグ メッセージを表示します。
	read	指定されたエラーテスト (1 、 2 、 3 、または 4) に関するファイル読み取り動作のデバッグメッセージを表示します。
	write	ファイル書き込み動作のデバッグ メッセージを表示します。

Command Default デバッグはディセーブルです。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **undebug sw-vlan ifs** コマンドは **no debug sw-vlan ifs** コマンドと同じです。

ファイルの読み取り処理に処理 **1** を選択すると、ヘッダー検証ワードおよびファイルバージョン番号が格納されたファイルヘッダーが読み込まれます。処理 **2** を指定すると、ドメインおよび VLAN 情報の大部分が格納されたファイル本体が読み取られます。処理 **3** を指定すると、Type Length Version (TLV) 記述子構造が読み取られます。処理 **4** を指定すると、TLV データが読み取られます。

Examples 次の例では、ファイル書き込み動作のデバッグ メッセージを表示する方法を示します。

```
Device> enable
Device# debug sw-vlan ifs write
```

debug sw-vlan notification

VLAN マネージャ通知のデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan notification** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}
no debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

Syntax Description	
accfwdchange	集約アクセスインターフェイススパニングツリー転送変更に関する VLAN マネージャ通知のデバッグメッセージを表示します。
allowedvlanfgchange	許可 VLAN の設定変更に関する VLAN マネージャ通知のデバッグメッセージを表示します。
fwdchange	スパニングツリー転送変更に関する VLAN マネージャ通知のデバッグメッセージを表示します。
linkchange	インターフェイスリンクステート変更の VLAN マネージャ通知のデバッグメッセージを表示します。
modechange	インターフェイスモード変更の VLAN マネージャ通知のデバッグメッセージを表示します。
pruningcfgchange	プルーニング設定変更の VLAN マネージャ通知のデバッグメッセージを表示します。
statechange	インターフェイスステート変更の VLAN マネージャ通知のデバッグメッセージを表示します。

Command Default デバッグはディセーブルです。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **undebg sw-vlan notification** コマンドは **no debug sw-vlan notification** コマンドと同じです。

あるスイッチスタック上でデバッグをイネーブルにした場合は、アクティブスイッチでのみイネーブルになります。特定のスタックメンバをデバッグする場合は、**session switch stack-member-number** 特権 EXEC コマンドを使用してアクティブスイッチから CLI セッションを開始できます。

Examples

次に、インターフェイスモード変更のVLANマネージャ通知のデバッグメッセージを表示する例を示します。

```
Device> enable
Device# debug sw-vlan notification
```

debug sw-vlan vtp

VLAN Trunking Protocol (VTP) コードのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan vtp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug sw-vlan vtp {events | packets | pruning [packets | xmit] | redundancy | xmit}
no debug sw-vlan vtp {events | packets | pruning | redundancy | xmit}
```

Syntax Description	events	汎用の論理フローのデバッグ メッセージおよび VTP コード内の VTP_LOG_RUNTIME マクロによって生成された VTP メッセージの詳細を表示します。
	packets	Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP パケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。
	pruning	VTP コードのプルーニング セグメントによって生成されるデバッグ メッセージを表示します。
	packets	（任意）Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP プルーニング パケットの内容のデバッグ メッセージを表示します。
	xmit	（任意）VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケットの内容のデバッグ メッセージを表示します。
	redundancy	VTP 冗長性のデバッグ メッセージを表示します。
	xmit	VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。

Command Default デバッグはディセーブルです。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines **undebug sw-vlan vtp** コマンドは **no debug sw-vlan vtp** コマンドと同じです。

pruning キーワードの後に追加のパラメータを入力しない場合は、VTP プルーニング デバッグ メッセージが表示されます。これらのメッセージは、VTP プルーニング コード内の

VTP_PRUNING_LOG_NOTICE、VTP_PRUNING_LOG_INFO、VTP_PRUNING_LOG_DEBUG、VTP_PRUNING_LOG_ALERT、および VTP_PRUNING_LOG_WARNING マクロによって生成されます。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。特定のスタックメンバをデバッグする場合は、**session switch** *stack-member-number* 特権 EXEC コマンドを使用してアクティブスイッチから CLI セッションを開始できます。

Examples

次に、VTP 冗長性のデバッグ メッセージを表示する例を示します。

```
Device> enable
Device# debug sw-vlan vtp redundancy
```

private-vlan

プライベート VLAN を設定し、プライマリプライベート VLAN とセカンダリ VLAN 間のアソシエーションを設定するには、スイッチスタックまたはスタンドアロンスイッチ上で **private-vlan** VLAN コンフィギュレーションコマンドを使用します。通常の VLAN 設定に VLAN を戻すには、このコマンドの **no** 形式を使用します。

```
private-vlan {association [add | remove] secondary-vlan-list | community | isolated | primary}
no private-vlan {association | community | isolated | primary}
```

Syntax Description	
association	プライマリ VLAN とセカンダリ VLAN とのアソシエーションを作成します。
add	セカンダリ VLAN をプライマリ VLAN に関連付けます。
remove	セカンダリ VLAN とプライマリ VLAN 間のアソシエーションをクリアします。
<i>secondary-vlan-list</i>	プライベート VLAN 内のプライマリ VLAN に対応させる 1 つまたは複数のセカンダリ VLAN。
community	VLAN をコミュニティ VLAN として指定します。
isolated	VLAN を独立 VLAN として指定します。
primary	VLAN をプライマリ VLAN として指定します。

Command Default デフォルトでは、プライベート VLAN が設定されていません。

Command Modes VLAN コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines プライベート VLAN を設定する前に、VLAN Trunking Protocol (VTP) をディセーブル (VTP トランスペアレントモード) にする必要があります。プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバに変更できません。

VTP は、プライベート VLAN の設定を伝播しません。レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定して、レイヤ 2 データベースを結合し、プライベート VLAN トラフィックのフラッドを防ぐ必要があります。

プライベート VLAN には、VLAN 1 または VLAN 1002 ~ 1005 を設定できません。拡張 VLAN (VLAN ID 1006 ~ 4094) はプライベート VLAN に設定できます。

セカンダリ（独立またはコミュニティ）VLAN を1つのプライマリ VLAN だけに対応させることができます。プライマリ VLAN には、1つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。

- セカンダリ VLAN をプライマリ VLAN として設定できません。
- *secondary-vlan-list* には、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。リストには、1つの独立 VLAN と複数のコミュニティ VLAN を含めることができます。
- プライマリまたはセカンダリ VLAN のいずれかを削除すると、VLAN に関連付けられたポートが非アクティブになります。

コミュニティ VLAN は、コミュニティ ポート間、およびコミュニティ ポートから対応するプライマリ VLAN の無差別ポートにトラフィックを伝送します。

独立 VLAN は、無差別ポートと通信を行うために独立ポートによって使用されます。同一のプライマリ VLAN ドメインで他のコミュニティ ポートまたは独立ポートにトラフィックを伝送しません。

プライマリ VLAN は、ゲートウェイからプライベート ポートのカスタマー エンドステーションにトラフィックを伝送する VLAN です。

レイヤ3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI はアクティブになりません。

VLAN コンフィギュレーションモードを終了するまで、**private-vlan** コマンドは作用しません。

プライベート VLAN ポートを EtherChannel として設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定はいずれも非アクティブです。

プライベート VLAN をリモート スイッチド ポート アナライザ（RSPAN）VLAN として設定しないでください。

プライベート VLAN を音声 VLAN として設定しないでください。

プライベート VLAN が設定されたスイッチにフォールバックブリッジングを設定しないでください。

プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行されるのは1つの STP インスタンスだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。

プライベート VLAN の他の機能との相互作用に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、VLAN 20 をプライマリ VLAN に、VLAN 501 を独立 VLAN に、VLAN 502 および 503 をコミュニティ VLAN に設定し、プライベート VLAN に関連付ける方法を示します。

```
デバイス# configure terminal  
デバイス(config)# vlan 20  
デバイス(config-vlan)# private-vlan primary  
デバイス(config-vlan)# exit  
デバイス(config)# vlan 501  
デバイス(config-vlan)# private-vlan isolated  
デバイス(config-vlan)# exit  
デバイス(config)# vlan 502  
デバイス(config-vlan)# private-vlan community  
デバイス(config-vlan)# exit  
デバイス(config)# vlan 503  
デバイス(config-vlan)# private-vlan community  
デバイス(config-vlan)# exit  
デバイス(config)# vlan 20  
デバイス(config-vlan)# private-vlan association 501-503  
デバイス(config-vlan)# end
```

設定を確認するには、**show vlan private-vlan** または **show interfaces status privileged EXEC** コマンドを入力します。

private-vlan mapping

両方の VLAN で同じプライマリ VLAN スイッチ仮想インターフェイス (SVI) を共有できるように、プライマリ VLAN とセカンダリ VLAN 間のマッピングを作成するには、スイッチ仮想インターフェイス (SVI) で **private-vlan mapping** インターフェイス コンフィギュレーション コマンドを使用します。SVI からプライベート VLAN のマッピングを削除するには、このコマンドの **no** 形式を使用します。

```
private-vlan mapping [add | remove] secondary-vlan-list
no private-vlan mapping
```

Syntax Description	add	(任意) セカンダリ VLAN をプライマリ VLAN SVI にマッピングします。
	remove	(任意) セカンダリ VLAN とプライマリ VLAN SVI 間のマッピングを削除します。
	<i>secondary-vlan-list</i>	(任意) 1 つまたは複数のセカンダリ VLAN をプライマリ VLAN SVI にマッピングします。
Command Default	プライベート VLAN SVI マッピングは設定されません。	
Command Modes	インターフェイス コンフィギュレーション	
Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Usage Guidelines	プライベート VLAN を設定する場合は、デバイスが VTP トランスペアレントモードになっている必要があります。	
	プライマリ VLAN の SVI は、レイヤ 3 で作成されます。	
	レイヤ 3 VLAN インターフェイス (SVI) はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI はアクティブになりません。	
	<i>secondary-vlan-list</i> 引数にスペースを含めることはできません。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。リストには、1 つの独立 VLAN と複数のコミュニティ VLAN を含めることができます。	
	セカンダリ VLAN で受信されたトラフィックは、プライマリ VLAN の SVI によってルーティングされます。	
セカンダリ VLAN は、1 つのプライマリ SVI だけにマッピングできます。プライマリ VLAN がセカンダリ VLAN として設定されると、このコマンドで指定されたすべての SVI はダウンします。		

有効なレイヤ2プライベートVLANのアソシエーションがない2つのVLAN間のマッピングを設定する場合、マッピングの設定は作用しません。

Examples

次の例では、VLAN 20のインターフェイスをVLAN 18のSVIにマッピングする方法を示します。

```
Device# configure terminal
Device# interface vlan 18
Device(config-if)# private-vlan mapping 20
Device(config-vlan)# end
```

次の例では、セカンダリVLAN 303～305、および307からのセカンダリVLANトラフィックのルーティングをVLAN 20 SVIを介して許可する方法を示します。

```
Device# configure terminal
Device# interface vlan 20
Device(config-if)# private-vlan mapping 303-305, 307
Device(config-vlan)# end
```

設定を確認するには、**show interfaces private-vlan mapping** 特権 EXEC コマンドを入力します。

show interfaces private-vlan mapping

VLAN スイッチ仮想インターフェイス（SVI）のプライベート VLAN のマッピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show interfaces private-vlan mapping** コマンドを使用します。

show interfaces [*interface-id*] **private-vlan mapping**

Syntax Description	<i>interface-id</i> （任意）プライベート VLAN のマッピング情報を表示するインターフェイスの ID。				
Command Default	なし				
Command Modes	ユーザ EXEC 特権 EXEC				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Examples

次に、プライベート VLAN のマッピングに関する情報を表示する例を示します。

```
Device#show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan2          301          community
vlan3          302          community
```

show vlan

設定されたすべての VLAN またはスイッチ上の 1 つの VLAN（VLAN ID または名前を指定した場合）のパラメータを表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan [**brief** | **group** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **private-vlan** [**type**] | **remote-span** | **summary**]

Syntax Description		
brief		（任意）VLAN ごとに VLAN 名、ステータス、およびポートを 1 行で表示します。
group		（任意）VLAN グループについての情報を表示します。
id <i>vlan-id</i>		（任意）VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。 <i>vlan-id</i> に指定できる範囲は 1 ～ 4094 です。
mtu		（任意）VLAN のリストと、VLAN のポートに設定されている最小および最大伝送単位（MTU）サイズを表示します。
name <i>vlan-name</i>		（任意）VLAN 名で特定された 1 つの VLAN に関する情報を表示します。VLAN 名は、1 ～ 32 文字の ASCII 文字列です。
private-vlan		（任意）プライマリおよびセカンダリ VLANID、タイプ（コミュニティ、独立、またはプライマリ）、およびプライベート VLAN に属するポートを含む、設定済みのプライベート VLAN の情報を表示します。このキーワードは、スイッチが IP サービスフィーチャセットを実行している場合にだけサポートされます。
type		（任意）プライベート VLAN ID およびタイプだけを表示します。
remote-span		（任意）Remote SPAN（RSPAN）VLAN に関する情報を表示します。
summary		（任意）VLAN サマリー情報を表示します。



Note **ifindex** キーワードは、コマンドラインのヘルプストリングに表示されますが、サポートされていません。

Command Modes ユーザ EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

show vlan mtu コマンド出力では、MTU_Mismatch 列に VLAN 内のすべてのポートに同じ MTU があるかどうかを示します。この列に **yes** が表示されている場合、VLAN の各ポートに別々の MTU があり、パケットが、大きい MTU を持つポートから小さい MTU を持つポートにスイッチングされると、ドロップされることがあります。VLAN に SVI がいない場合、ハイフン (-) 記号が SVI_MTU 列に表示されます。MTU-Mismatch 列に **yes** が表示されている場合、MiniMTU と MaxMTU を持つポート名が表示されます。

セカンダリ VLAN を定義する前にプライベート VLAN のセカンダリ VLAN をプライマリ VLAN に対応させようとする、セカンダリ VLAN が **show vlan private-vlan** コマンドの出力に含まれません。

show vlan private-vlan type コマンドの出力では、**normal** として表示されたタイプは、プライベート VLAN のアソシエーションを持っていても、プライベート VLAN の一部ではない VLAN であることを意味します。たとえば、2つの VLAN をプライマリ VLAN およびセカンダリ VLAN と定義し、対応させた後で、プライマリ VLAN からアソシエーションを削除せずにセカンダリ VLAN の設定を削除した場合、セカンダリ VLAN だった VLAN が出力に **normal** として表示されます。

show vlan private-vlan 出力では、プライマリとセカンダリ VLAN のペアが **nonoperational** と表示されます。

Examples

次に、**show vlan** コマンドの出力例を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show vlan
VLAN Name                Status      Ports
-----
1    default                active     Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7
                                           Gi1/0/8, Gi1/0/9, Gi1/0/10
                                           Gi1/0/11, Gi1/0/12, Gi1/0/13
                                           Gi1/0/14, Gi1/0/15, Gi1/0/16
                                           Gi1/0/17, Gi1/0/18, Gi1/0/19
                                           Gi1/0/20, Gi1/0/21, Gi1/0/22
                                           Gi1/0/23, Gi1/0/24, Gi1/0/25
                                           Gi1/0/26, Gi1/0/27, Gi1/0/28
                                           Gi1/0/29, Gi1/0/30, Gi1/0/31
                                           Gi1/0/32, Gi1/0/33, Gi1/0/34
                                           Gi1/0/35, Gi1/0/36, Gi1/0/37
                                           Gi1/0/38, Gi1/0/39, Gi1/0/40
                                           Gi1/0/41, Gi1/0/42, Gi1/0/43
                                           Gi1/0/44, Gi1/0/45, Gi1/0/46
                                           Gi1/0/47, Gi1/0/48

2    VLAN0002                active
40   vlan-40                  active
300  VLAN0300                 active
1002 fddi-default            act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default          act/unsup

VLAN Type  SAID          MTU    Parent RingNo BridgeNo Stp   BrdgMode Trans1 Trans2
-----

```

```

1   enet  100001   1500 -   -   -   -   -   0   0
2   enet  100002   1500 -   -   -   -   -   0   0
40  enet  100040   1500 -   -   -   -   -   0   0
300 enet  100300   1500 -   -   -   -   -   0   0
1002 fddi  101002   1500 -   -   -   -   -   0   0
1003 tr    101003   1500 -   -   -   -   -   0   0
1004 fdnet 101004   1500 -   -   -   ieee -   0   0
1005 trnet 101005   1500 -   -   -   ibm  -   0   0
2000 enet  102000   1500 -   -   -   -   -   0   0
3000 enet  103000   1500 -   -   -   -   -   0   0

```

Remote SPAN VLANs

2000,3000

Primary Secondary Type Ports

Table 170: show vlan コマンドの出力フィールド

フィールド	説明
VLAN	VLAN 番号。
Name	VLAN の名前（設定されている場合）。
Status	VLAN のステータス（active または suspend）。
Ports	VLAN に属するポート。
Type	VLAN のメディア タイプ。
SAID	VLAN のセキュリティ アソシエーション ID 値。
MTU	VLAN の最大伝送単位サイズ。
Parent	親 VLAN（存在する場合）。
RingNo	VLAN のリング番号（該当する場合）。
BrdgNo	VLAN のブリッジ番号（該当する場合）。
Stp	VLAN で使用されるスパニングツリープロトコル タイプ。
BrdgMode	この VLAN のブリッジング モード：可能な値はソースルートブリッジング（SRB）およびソースルートトランスペアレント（SRT）で、デフォルトは SRB です。
Trans1	トランスレーションブリッジ 1。
Trans2	トランスレーションブリッジ 2。
Remote SPAN VLANs	設定されている RSPAN VLAN を識別します。

次に、**show vlan summary** コマンドの出力例を示します。

```
Device> show vlan summary
Number of existing VLANs           : 45
Number of existing VTP VLANs      : 45
Number of existing extended VLANs : 0
```

次に、**show vlan id** コマンドの出力例を示します。

```
Device# show vlan id 2
VLAN Name                Status      Ports
-----
2    VLAN0200                active     Gi1/0/7, Gi1/0/8
2    VLAN0200                active     Gi2/0/1, Gi2/0/2

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
2    enet    100002   1500   -      -      -    -    -      0      0

Remote SPAN VLANs
-----
Disabled
```

show vtp

VLAN Trunking Protocol (VTP) 管理ドメイン、ステータス、およびカウンタに関する一般情報を表示するには、EXEC モードで **show vtp** コマンドを使用します。

show vtp {**counters** | **devices** [**conflicts**] | **interface** [*interface-id*] | **password** | **status**}

Syntax Description

counters	デバイスの VTP 統計情報を表示します。
devices	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。このキーワードは、デバイスが VTP バージョン 3 を実行していない場合だけ適用されます。
conflicts	(任意) 競合するプライマリ サーバを持つ VTP バージョン 3 デバイスに関する情報を表示します。デバイスが VTP トランスペアレントモードまたは VTP オフモードにある場合、このコマンドは無視されます。
interface	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
<i>interface-id</i>	(任意) VTP ステータスおよび設定を表示するインターフェイス。ここには物理インターフェイスまたはポート チャネルを指定できます。
password	VTP パスワードが設定されているかどうかを表示します (特権 EXEC モードでのみ使用可能)。
status	VTP 管理ドメインのステータスに関する一般情報を表示します。

Command Modes

ユーザ EXEC

特権 EXEC

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.12.4	show vtp password コマンドの出力は、パスワードが設定されているかどうかを表示します。

Examples

次に、**show vtp devices** コマンドの出力例を示します。**Conflict** 列の **Yes** は、応答するサーバがその機能のローカルサーバと競合していることを示します。つまり、同じドメイン内の 2 つのデバイスは、データベースに対して同じプライマリサーバを持ちません。

```
Device> enable
Device# show vtp devices
```

```
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf Device ID      Primary Server Revision  System Name
-----
VLAN      Yes  00b0.8e50.d000  000c.0412.6300  12354      main.cisco.com
MST       No   00b0.8e50.d000  0004.AB45.6000  24         main.cisco.com
VLAN      Yes  000c.0412.6300=000c.0412.6300  67         qwerty.cisco.com
```

次に、**show vtp counters** コマンドの出力例を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Device> show vtp counters
VTP statistics:
Summary advertisements received      : 0
Subset advertisements received      : 0
Request advertisements received      : 0
Summary advertisements transmitted  : 0
Subset advertisements transmitted    : 0
Request advertisements transmitted   : 0
Number of config revision errors     : 0
Number of config digest errors       : 0
Number of V1 summary errors          : 0

VTP pruning statistics:

Trunk      Join Transmitted Join Received      Summary advts received from
-----
Gi1/0/47   0                0                  0
Gi1/0/48   0                0                  0
Gi2/0/1    0                0                  0
Gi3/0/2    0                0                  0
```

Table 171: show vtp counters のフィールドの説明

フィールド	説明
Summary advertisements received	トランクポート上でこのデバイスが受信するサマリーアドバタイズメントの数。サマリーアドバタイズには、管理ドメイン名、コンフィギュレーションリビジョン番号、更新タイムスタンプとID、認証チェックサム、および関連するサブセットアドバタイズの数が含まれます。
Subset advertisements received	トランクポート上でこのデバイスが受信するサブセットアドバタイズメントの数。サブセットアドバタイズには、1つ以上のVLANに関する情報がすべて含まれています。
Request advertisements received	トランクポート上でこのデバイスが受信するアドバタイズメント要求の数。アドバタイズ要求は、通常、すべてのVLAN上に関する情報を要求します。また、VLANのサブセットに関する情報も要求できます。

フィールド	説明
Summary advertisements transmitted	トランクポート上でこのデバイスが送信するサマリーアドバタイズメントの数。サマリーアドバタイズには、管理ドメイン名、コンフィギュレーションリビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセットアドバタイズの数が含まれます。
Subset advertisements transmitted	トランクポート上でこのデバイスが送信するサブセットアドバタイズメントの数。サブセットアドバタイズには、1つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements transmitted	トランクポート上でこのデバイスが送信するアドバタイズメント要求の数。アドバタイズ要求は、通常、すべての VLAN に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Number of configuration revision errors	<p>リビジョンエラーの数。</p> <p>新しい VLAN の定義、既存 VLAN の削除、中断、または再開、あるいは既存 VLAN のパラメータ変更を行うと、デバイスのコンフィギュレーションリビジョン番号が増加します。</p> <p>リビジョン番号がデバイスのリビジョン番号と一致するにもかかわらず、MD5 ダイジェスト値が一致しないアドバタイズメントをデバイスが受信すると、リビジョンエラーが増加します。このエラーは、2つのデバイスの VTP パスワードが異なるか、またはデバイスの設定が異なることを意味します。</p> <p>これらのエラーは、デバイスが受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。</p>

フィールド	説明
Number of configuration digest errors	<p>MD5 ダイジェスト エラーの数。</p> <p>サマリーパケット内の MD5 ダイジェストと、デバイスによって計算された受信済みアドバタイズメントの MD5 ダイジェストが一致しない場合は、ダイジェストエラーが増加します。このエラーは、通常、2つのデバイスの VTP パスワードが異なることを意味します。この問題を解決するには、すべてのデバイスで VTP パスワードが同じになるようにします。</p> <p>これらのエラーは、デバイスが受信アドバタイズメントをフィルタして、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。</p>
Number of V1 summary errors	<p>バージョン 1 エラーの数。</p> <p>VTP V2 モードのデバイスが VTP バージョン 1 フレームを受信すると、バージョン 1 サマリーエラーが増加します。これらのエラーは、少なくとも1つの近接デバイスで、V2モードがディセーブルにされた VTP バージョン 1、または VTP バージョン 2 が実行されていることを示しています。この問題を解決するには、VTP V2 モードのデバイスの設定をディセーブルに変更します。</p>
Join Transmitted	トランク上で送信された VTP プルーニングメッセージの数。
Join Received	トランク上で受信された VTP プルーニングメッセージの数。
Summary Advts Received from non-pruning-capable device	トランク上で受信された、プルーニングをサポートしていないデバイスからの VTP サマリーメッセージの数。

次に、**show vtp status** コマンドの出力例を示します。次の表に、この出力で表示される各フィールドについて説明します。

```

Device> show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 1
VTP Domain Name         :
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02

```

```
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)
```

```
Feature VLAN:
```

```
-----
VTP Operating Mode           : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs     : 7
Configuration Revision       : 2
MD5 digest                   : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                               0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

Table 172: show vtp status のフィールドの説明

フィールド	説明
VTP Version capable	デバイス上で動作できる VTP バージョンを表示します。
VTP Version running	デバイス上で動作中の VTP バージョンを表示します。デフォルトでは、デバイスはバージョン 1 を実行しますが、バージョン 2 に設定することもできます。
VTP Domain Name	デバイスの管理ドメインを特定する名前。
VTP Pruning Mode	プルーニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。プルーニングを使用すると、トラフィックが適切なネットワークデバイスにアクセスするために使用しなければならないトランクリンクへのフラッドイングトラフィックが制限されます。
VTP Traps Generation	VTP トラップをネットワーク管理ステーションに送信するかどうかを表示します。
Device ID	ローカル デバイスの MAC アドレスを表示します。
Configuration last modified	最後に行った設定変更の日付と時刻を表示します。データベースの設定変更の原因となったデバイスの IP アドレスを表示します。

フィールド	説明
VTP Operating Mode	<p>VTP 動作モード（サーバ、クライアント、またはトランスペアレント）を表示します。</p> <p>Server: VTP サーバモードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信します。スイッチで VLAN を設定できます。このデバイスを使用すると、起動後に、現在の VTP データベース内のすべての VLAN 情報を、NVRAM から復元できます。デフォルトでは、すべてのデバイスが VTP サーバです。</p> <p>Note デバイスが設定を NVRAM に書き込んでいる間に障害を検出し、NVRAM が機能するまでサーバモードに戻るできない場合、スイッチは VTP サーバモードから VTP クライアントモードに自動的に変わります。</p> <p>Client: VTP クライアントモードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するために十分な不揮発性ストレージがありません。スイッチでは VLAN を設定できません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。</p> <p>Transparent: VTP トランスペアレントモードのデバイスは、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定にも影響しません。デバイスは VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランクポートを除くすべてのトランクポートにこれを転送します。</p>
Maximum VLANs Supported Locally	ローカルにサポートされている VLAN の最大数。
Number of Existing VLANs	既存の VLAN 数。
Configuration Revision	このデバイスの現在のコンフィギュレーションリビジョン番号。

フィールド	説明
MD5 Digest	VTP 設定の 16 バイト チェックサム。

switchport mode private-vlan

インターフェイスをホストプライベート VLAN ポートまたは無差別プライベート VLAN ポートとして設定するには、インターフェイス コンフィギュレーション モードで **switchport mode private-vlan** コマンドを使用します。モードをデバイスに適したデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

```
switchport mode private-vlan {host | promiscuous}
no switchport mode private-vlan
```

Syntax Description	<p>host インターフェイスをプライベート VLAN ホスト ポートとして設定します。ホストポートはプライベート VLAN のセカンダリ VLAN に所属しており、所属する VLAN に応じてコミュニティ ポートまたは独立ポートのいずれかになります。</p> <p>promiscuous インターフェイスをプライベート VLAN 無差別ポートとして設定します。無差別ポートは、プライベート VLAN のプライマリ VLAN のメンバです。</p>				
Command Default	なし				
Command Modes	インターフェイス コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				

Usage Guidelines プライベート VLAN のホストポートまたは無差別ポートは、スイッチドポートアナライザ (SPAN) 宛先ポートには設定できません。SPAN 宛先ポートをプライベート VLAN のホストポートまたは無差別ポートとして設定する場合、ポートが非アクティブになります。

ポート上のプライベート VLAN に他の機能 (以下) を設定しないでください。

- ダイナミック アクセス ポート VLAN メンバーシップ
- ダイナミック トランキング プロトコル (DTP)
- ポート集約プロトコル (PAgP)
- リンク集約制御プロトコル (LACP)
- マルチキャスト VLAN レジストレーション (MVR)
- 音声 VLAN

ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定はいつでも非アクティブです。

プライベート VLAN ポートはセキュアポートにはできないので、保護ポートとして設定できません。

プライベート VLAN の他の機能との相互作用に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

設定の矛盾による STP ループの発生を防ぎ、STP コンバージェンスをより速く行うために、独立およびコミュニティ ホストポート上でスパニングツリー PortFast およびブリッジプロトコルデータ ユニット (BPDU) ガードをイネーブルにすることを強く推奨します。

ポートをプライベート VLAN ホストポートとして設定し、**switchport private-vlan host-association** コマンドを使用して有効なプライベート VLAN のアソシエーションを設定しない場合、インターフェイスは非アクティブになります。

ポートをプライベート VLAN 無差別ポートとして設定し、**switchport private-vlan mapping** コマンドを使用して有効なプライベート VLAN のマッピングを設定しない場合、インターフェイスは非アクティブになります。

Examples

次の例では、インターフェイスをプライベート VLAN ホストポートとして設定し、それをプライマリ VLAN 20 に関連付ける方法を示します。インターフェイスは、セカンダリ独立 VLAN 501 およびプライマリ VLAN 20 のメンバです。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# switchport mode private-vlan host
デバイス (config-if)# switchport private-vlan host-association 20 501
デバイス (config-if)# end
```

次に、インターフェイスをプライベート VLAN 無差別ポートとして設定してそれをプライベート VLAN にマッピングする例を示します。インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ~ 503 がマッピングされます。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# switchport mode private-vlan promiscuous
デバイス (config-if)# switchport private-vlan mapping 20 501-503
デバイス (config-if)# end
```

switchport priority extend

着信したタグなしフレームのポートプライオリティ、または指定されたポートに接続された IP フォンが受信するフレームのプライオリティを設定するには、インターフェイス コンフィギュレーションモードで **switchport priority extend** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport priority extend {cos value | trust}
no switchport priority extend
```

Syntax Description	<p>cos value PCから受信したか、または指定した Class of Service (CoS) 値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は 0 ~ 7 です。7 が最も高いプライオリティです。デフォルトは 0 です。</p> <p>trust PCまたは接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。</p>				
Command Default	ポートで受信したタグなしフレームには、デフォルトポートプライオリティは、CoS 値 0 で設定されています。				
Command Modes	インターフェイス コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	<p>音声 VLAN をイネーブルにした場合、デバイスを設定して、Cisco Discovery Protocol (CDP) パケットを送信し、Cisco IP 電話のアクセスポートに接続される装置からデータパケットを送信する方法を IP 電話に指示できます。Cisco IP 電話に設定を送信するには、Cisco IP 電話に接続しているデバイスポートの CDP をイネーブルにする必要があります (デフォルトでは、CDP はすべてのデバイスインターフェイスでグローバルにイネーブルです)。</p> <p>デバイスアクセスポート上で音声 VLAN を設定する必要があります。</p> <p>次の例では、受信した IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。</p> <pre>Device> enable Device# configure terminal Device(config)# interface gigabitethernet1/0/2 Device(config-if)# switchport priority extend trust</pre> <p>設定を確認するには、show interfaces interface-id switchport 特権 EXEC コマンドを入力します。</p>				

switchport trunk

インターフェイスがトランキングモードの場合、トランクの特性を設定するには、インターフェイス コンフィギュレーション モードで **switchport trunk** コマンドを使用します。トランキング特性をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

```
switchport trunk {allowed vlan vlan-list | native vlan vlan-id | pruning vlan vlan-list }
no switchport trunk {allowed vlan | native vlan | pruning vlan }
```

Syntax Description	
allowed vlan <i>vlan-list</i>	トランキングモードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可VLANのリストを設定します。 <i>vlan-list</i> の選択については、「使用上のガイドライン」を参照してください。
native vlan <i>vlan-id</i>	インターフェイスが IEEE 802.1Q トランキング モードの場合に、タグなしトラフィックを送受信するようにネイティブVLANを設定します。指定できる範囲は1～4094です。
pruning vlan <i>vlan-list</i>	トランキング モードの場合に、VTP プルーニングに適格なVLANのリストを設定します。 <i>vlan-list</i> の選択については、「使用上のガイドライン」を参照してください。

Command Default VLAN 1 は、ポートのデフォルトのネイティブ VLAN ID です。
すべての VLAN リストのデフォルトには、すべての VLAN が含まれます。

Command Modes インターフェイス コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines *vlan-list* の形式は、**all | none | [add | remove | except] *vlan-atom* [,*vlan-atom*...]** です。:

- **all** 1～4094のすべてのVLANを指定します。これはデフォルトです。このキーワードは、リストのすべてのVLANを同時に設定することを許可しないコマンド上では使用できません。
- **none** 空のリストを指定します。特定のVLANを設定するか、または少なくとも1つのVLANを設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** リストを置き換えるのではなく、現在設定されているVLANにVLANの定義済みリストを追加します。有効なIDは1～1005です。場合によっては、拡張範囲VLAN（VLAN IDが1005より上）を使用できます。



Note 許可 VLAN リストに拡張範囲 VLAN を追加できますが、プルーニング適格 VLAN リストには追加できません。

カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。

- **remove** リストを置き換えるのではなく、現在設定されている VLAN から VLAN の定義済みリストを削除します。有効な ID は 1 ~ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。



Note 許可 VLAN リストから拡張範囲 VLAN を削除できますが、プルーニング適格リストからは削除できません。

- **except** 定義済み VLAN リスト以外の、計算する必要がある VLAN を示します（指定されている VLAN 以外の VLAN が追加されます）。有効な ID の範囲は 1 ~ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **vlan-atom** は、1 ~ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、小さい方の値を先頭にハイフンで区切ります。

ネイティブ VLAN:

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブモード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN:

- スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol (CDP)、ポート集約プロトコル (PAgP)、Link Aggregation Control Protocol (LACP)、ダイナミック トランッキング プロトコル (DTP)、および VLAN 1 の VLAN トランッキング プロトコル (VTP)) を送受信し続けます。
- **allowed vlan** コマンドの **no** 形式は、リストをデフォルトリスト（すべての VLAN を許可）にリセットします。

トランク プルーニング:

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLAN をプルーニングしない場合は、プルーニング適格リストから VLAN を削除します。プルーニング不適格の VLAN は、フラッドイング トラフィックを受信します。
- VLAN 1、VLAN 1002 ~ 1005、および拡張範囲 VLAN (VLAN 1006 ~ 4094) は、プルーニングできません。

Examples

次の例では、すべてのタグなしトラフィックを送信するポートのデフォルトとして、VLAN 3 を設定する方法を示します。

```
Device> enable
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk native vlan 3
```

次の例では、許可リストに VLAN 1、2、5、および 6 を追加する方法を示します。

```
Device> enable
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ~ 15 を削除する方法を示します。

```
Device> enable
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk pruning vlan remove 3,10-15
```

設定を確認するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを入力します。

vlan

VLANを追加して、VLAN コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

```
vlan vlan-id
no vlan vlan-id
```

Syntax Description	<i>vlan-id</i> 追加および設定する VLAN の ID。指定できる範囲は 1 ~ 4094 です。1 つの VLAN ID、それぞれをカンマで区切った一連の VLAN ID、またはハイフンを間に挿入した VLAN ID の範囲を入力できます。				
Command Default	なし				
Command Modes	グローバル コンフィギュレーション				
Command History	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。				
Usage Guidelines	<p>通常範囲の VLAN (VLAN ID 1 ~ 1005) や拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を追加するには、vlan vlan-id グローバルコンフィギュレーションコマンドを使用します。通常範囲の VLAN の設定情報は常に VLAN データベースに保存されます。この情報を表示するには、show vlan 特権 EXEC コマンドを入力します。VTP モードがトランスペアレントである場合、通常範囲の VLAN の VLAN 設定情報も device の実行コンフィギュレーションファイルに保存されます。拡張範囲の VLAN ID は VLAN データベースに保存されず、スイッチの実行コンフィギュレーションファイルに保存されます。また、設定をスタートアップコンフィギュレーションファイルに保存できます。</p> <p>VTP バージョン 3 は拡張範囲 VLAN の伝播をサポートしています。VTP バージョン 1 および 2 で伝播する範囲は、VLAN 1 ~ 1005 だけです。</p> <p>VLAN および VTP 設定をスタートアップコンフィギュレーションファイルに保存して device をリブートすると、設定は次のように選択されます。</p> <ul style="list-style-type: none"> スタートアップコンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップコンフィギュレーションファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され (クリアされ)、スタートアップコンフィギュレーションファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。 スタートアップコンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ~ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。 				

無効な VLAN ID を入力すると、エラーメッセージが表示され、VLAN コンフィギュレーションモードを開始できません。

VLANIDを指定して **vlan** コマンドを入力すると、VLAN コンフィギュレーションモードがイネーブルになります。既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更できます。指定された VLAN は、VLAN コンフィギュレーションモードを終了したときに追加または変更されます。（VLAN 1 ～ 1005 の）**shutdown** コマンドだけがただちに有効になります。



Note すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされる VLAN コンフィギュレーション コマンドは **remote-span** だけです。拡張範囲 VLAN の場合、他のすべての特性はデフォルト状態のままにしておく必要があります。

次のコンフィギュレーションコマンドを VLAN コンフィギュレーションモードで利用できます。各コマンドの **no** 形式を使用すると、特性がそのデフォルト状態に戻ります。

- **are are-number:** この VLAN の全ルート エクスプローラ (ARE) ホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。デフォルト値は 7 です。値が入力されない場合、最大数は 0 であると見なされます。
- **backupcrf:** バックアップ CRF モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。
 - **enable:** この VLAN のバックアップ CRF モード。
 - **disable:** この VLAN のバックアップ CRF モード (デフォルト)。
- **bridge {bridge-number |type}:** 論理分散ソースルーティングブリッジ、つまり、FDDI-NET、トークンリング NET、および TrBRF VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。指定できる範囲は 0 ～ 15 です。FDDI-NET、TrBRF、およびトークンリング NET VLAN については、デフォルトのブリッジ番号は 0 (ソースルーティングブリッジなし) です。 **type** キーワードは、TrCRF VLAN だけに適用され、次のうちのいずれかです。
 - **srb:** ソースルートブリッジング。
 - **srt:** (ソースルート トランスペアレント) ブリッジング VLAN
- **exit:** 変更を適用し、VLAN データベース リビジョン番号 (VLAN 1 ～ 1005) を増加させ、VLAN コンフィギュレーションモードを終了します。
- **media:** VLAN メディア タイプを定義します。タイプは次のいずれかになります。



Note device がサポートするのは、イーサネット ポートだけです。FDDI およびトークンリング メディア固有の特性は、別の devices に対する VLAN Trunking Protocol (VTP) グローバル アドバタイズメントに限って設定します。これらの VLAN はローカルに停止されます。

- **ethernet:** イーサネット メディア タイプ (デフォルト)。
- **fd-net:** FDDI ネットワーク エンティティ タイトル (NET) メディア タイプ。
- **fd-di:** FDDI メディア タイプ。
- **tokenring:** VTP v2 モードがディセーブルの場合は、トークンリング メディア タイプ。VTP バージョン 2 (v) モードがイネーブルの場合は、TrCRF。
- **tr-net:** VTP v2 モードがディセーブルの場合は、トークンリング ネットワーク エンティティ タイトル (NET) メディア タイプ。VTP v2 モードがイネーブルの場合は、TrBRF メディア タイプ。

さまざまなメディア タイプで有効なコマンドおよび構文については、下の表を参照してください。

- **name *vlan-name*:** 管理ドメイン内で一意である 1 ~ 32 文字の ASCII 文字列で VLAN に名前を付けます。デフォルトは VLANxxxx です。ここで、xxxx は VLAN ID 番号と同じ 4 桁の数字 (先行ゼロを含む) です。
- **no:** コマンドを無効にするか、またはデフォルト設定に戻します。
- **parent *parent-vlan-id*:** 既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定しますこのパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときが必要です。指定できる範囲は 0 ~ 1005 です。デフォルトの親 VLAN ID は、FDDI およびトークンリング VLAN では 0 (親 VLAN なし) です。トークンリングおよび TrCRF VLAN の両方で、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。
- **remote-span:** VLAN をリモート SPAN (RSPAN) VLAN として設定します。RSPAN 機能が既存の VLAN に追加される場合、まず VLAN は削除され、次に RSPAN 機能とともに再生されます。RSPAN 機能が削除されるまで、どのアクセス ポートも非アクティブになります。VTP がイネーブルの場合、新しい RSPAN VLAN は、1024 より小さい数字の VLAN ID の VTP により伝播されます。ラーニングは VLAN 上でディセーブルになります。
- **ring *ring-number*:** FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる範囲は 1 ~ 4095 です。トークンリング VLAN のデフォルト値は 0 です。FDDI VLAN には、デフォルト設定はありません。
- **said *said-value*:** IEEE 802.10 に記載されているセキュリティ アソシエーション ID (SAID) を指定します。指定できる ID は、1 ~ 4294967294 です。この数字は、管理ドメイン内で一意である必要があります。デフォルト値は、100000 に VLAN ID 番号を加算した値です。

- **shutdown:** VLAN 上で VLAN スイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、VLAN コンフィギュレーションモードを終了したときに有効になります。
- **state:** VLAN の状態を指定します。
 - **active** VLAN が稼働中であることを意味します（デフォルト）。
 - **suspend** VLAN が停止していることを意味します。停止している VLAN はパケットを通過させません。
- **ste ste-number:** スパニングツリーエクスプローラ（STE）ホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0～13 です。デフォルト値は 7 です。
- **stp type:** FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニングツリータイプを定義します。FDDI-NET VLAN の場合、デフォルトの STP タイプは **ieee** です。トークンリング NET VLAN の場合、デフォルトの STP タイプは **ibm** です。FDDI およびトークンリング VLAN の場合、デフォルトのタイプは指定されていません。
 - **ieee:** ソースルートトランスペアレント（SRT）ブリッジングを実行している IEEE イーサネット STP。
 - **ibm:** ソースルートブリッジング（SRB）を実行している IBM STP。
 - **auto:** ソースルートトランスペアレント（SRT）ブリッジング（IEEE）およびソースルートブリッジング（IBM）の組み合わせを実行している STP。
- **tb-vlan1 tb-vlan1-id** および **tb-vlan2 tb-vlan2-id:** この VLAN にトランスレーショナルブリッジングが行われている 1 番めおよび 2 番めの VLAN を指定します。トランスレーショナル VLAN は、たとえば FDDI またはトークンリングをイーサネットに変換します。指定できる範囲は 0～1005 です。値が指定されないと、0（トランスレーショナルブリッジングなし）と見なされます。

Table 173: さまざまなメディアタイプで指定できるコマンドと構文

メディアタイプ	指定できる構文
イーサネット	name <i>vlan-name</i> , media ethernet , state { suspend active }, said <i>said-value</i> , remote-span , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI	name <i>vlan-name</i> , media fddi , state { suspend active }, said <i>said-value</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>

メディアタイプ	指定できる構文
FDDI-NET	<p>name <i>vlan-name</i>, media fd-net, state {suspend active}, said <i>said-value</i>, bridge <i>bridge-number</i>, stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i>, tb-vlan2 <i>tb-vlan2-id</i></p> <p>VTP v2 モードがディセーブルの場合は、stp type を auto. に設定しないでください</p>
Token Ring	<p>VTP v1 モードはイネーブルです。</p> <p>name <i>vlan-name</i>, media tokenring, state {suspend active}, said <i>said-value</i>, ring <i>ring-number</i>, parent <i>parent-vlan-id</i>, tb-vlan1 <i>tb-vlan1-id</i>, tb-vlan2 <i>tb-vlan2-id</i></p>
トークンリング コンセントレータ リレー機能 (TrCRF)	<p>VTP v2 モードはイネーブルです。</p> <p>name <i>vlan-name</i>, media tokenring, state {suspend active}, said <i>said-value</i>, ring <i>ring-number</i>, parent <i>parent-vlan-id</i>, bridge type {srb srt}, are <i>are-number</i>, ste <i>ste-number</i>, backupcrf {enable disable}, tb-vlan1 <i>tb-vlan1-id</i>, tb-vlan2 <i>tb-vlan2-id</i></p>
トークンリング NET	<p>VTP v1 モードはイネーブルです。</p> <p>name <i>vlan-name</i>, media tr-net, state {suspend active}, said <i>said-value</i>, bridge <i>bridge-number</i>, stp type {ieee ibm}, tb-vlan1 <i>tb-vlan1-id</i>, tb-vlan2 <i>tb-vlan2-id</i></p>
トークンリングブリッジリレー機能 (TrBRF)	<p>VTP v2 モードはイネーブルです。</p> <p>name <i>vlan-name</i>, media tr-net, state {suspend active}, said <i>said-value</i>, bridge <i>bridge-number</i>, stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i>, tb-vlan2 <i>tb-vlan2-id</i></p>

次の表に、VLAN の設定ルールを示します。

Table 174: VLAN 設定ルール

設定	ルール
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	<p>すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。</p> <p>リング番号を指定します。このフィールドを空白のままにしないでください。</p> <p>TrCRF VLAN に同じ親 VLAN ID がある場合には一意のリング番号を指定します。1つのバックアップ コンセントレータリレー機能 (CRF) だけをイネーブルにすることができます。</p>
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしないでください。
VTP v1 モードがイネーブルの場合	<p>VLAN の STP タイプを auto に設定しないでください。</p> <p>このルールは、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。</p>

設定	ルール
<p>トランスレーショナルブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）</p>	<p>使用されるトランスレーショナルブリッジング VLANID は、すでにデータベースに存在している必要があります。</p> <p>（たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナルブリッジング VLAN ID にも、トランスレーショナルブリッジング パラメータの 1 つに元の VLAN へのポインタが含まれている必要があります。</p> <p>コンフィギュレーションがポイントするトランスレーショナルブリッジング VLANID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）元の VLAN とは異なるメディアタイプである必要があります。</p> <p>両方のトランスレーショナルブリッジング VLANID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なるメディアタイプである必要があります。</p>

Examples

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには VLAN *xxxx* の *vlan-name* が含まれています。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。デフォルトの *media* は *ethernet* です。*state* は *active* です。デフォルトの *said-value* は、100000 に VLAN ID を加算した値です。*mtu-size* 変数は 1500、*stp-type* は *ieee* です。**exit VLAN** コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何も作用しません。

次に、新しい VLAN をすべてデフォルトの特性で作成し、VLAN コンフィギュレーション モードを開始する例を示します。

```

デバイス(config)# vlan 200
デバイス(config-vlan)# exit
デバイス(config)#

```

次に、新しい拡張範囲 VLAN をすべてデフォルトの特性で作成して、VLAN コンフィギュレーションモードを開始し、新しい VLAN を *device* のスタートアップ コンフィギュレーション ファイルに保存する例を示します。

```
デバイス(config)# vlan 2000  
デバイス(config-vlan)# end  
デバイス# copy running-config startup config
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

vlan dot1q tag native

すべての IEEE 802.1Q トランクポートでネイティブ VLAN フレームのタグgingをイネーブルにするには、グローバル コンフィギュレーション モードで **vlan dot1q tag native** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
vlan dot1q tag native
no vlan dot1q tag native
```

Syntax Description

このコマンドには引数またはキーワードはありません。

Command Default

IEEE 802.1Q ネイティブ VLAN タグgingはディセーブルです。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

イネーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされます。

ディセーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされません。

IEEE 802.1Q トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

Examples

次の例では、ネイティブ VLAN フレームの IEEE 802.1Q タグgingをイネーブルにする方法を示します。

```
Device# configure terminal
Device (config)# vlan dot1q tag native
Device (config)# end
```

設定を確認するには、**show vlan dot1q tag native** 特権 EXEC コマンドを入力します。

vtp (グローバルコンフィギュレーション)

VLAN トランッキングプロトコル (VTP) 設定の特性を設定するか、または変更するには、グローバルコンフィギュレーションモードで **vtp** コマンドを使用します。この設定を削除したりデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
vtp {domain domain-name | file filename | interface interface-name [only] | mode {client | off | server | transparent} [mst | unknown | vlan] | password password [hidden | secret] | pruning | version number}
no vtp {file | interface | mode [client | off | server | transparent] [mst | unknown | vlan] | password | pruning | version}
```

Syntax Description

domain <i>domain-name</i>	VTP ドメイン名をデバイスの VTP 管理ドメインを識別する 1～32 文字の ASCII 文字列で指定します。ドメイン名では大文字と小文字が区別されます。
file <i>filename</i>	VTP VLAN 設定が保存されている Cisco IOS ファイルシステム ファイルを指定します。
interface <i>interface-name</i>	このデバイスで更新された VTP ID を提供するインターフェイスの名前を指定します。
only	(任意) VTP IP アップデータとしてこのインターフェイスの IP アドレスだけを使用します。
mode	VTP デバイスモードをクライアント、サーバ、またはトランスペアレントに指定します。
client	デバイスを VTP クライアントモードにします。VTP クライアントモードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するための十分な不揮発性メモリがありません。VTP クライアントでは、VLAN を設定できません。VLAN は、ドメインに含まれる、他のサーバモードのデバイスで設定します。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
off	デバイスを VTP オフモードにします。VTP オフモードのデバイスは、トランクポート上で VTP アドバタイズメントを転送しないことを除いて、VTP トランスペアレントデバイスと同様に機能します。
server	デバイスを VTP サーバモードにします。VTP サーバモードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信します。デバイスで VLAN を設定できます。デバイスは、再起動後に、不揮発性メモリから現在の VTP データベース内のすべての VLAN 情報を回復できます。

transparent	<p>デバイスを VTP トランスペアレントモードにします。VTP トランスペアレントモードのデバイスは、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントからの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定に影響を与えることはありません。デバイスは VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランクポートを除くすべてのトランクポートにこれを転送します。</p> <p>VTP モードがトランスペアレントである場合、モードおよびドメイン名はデバイスの実行コンフィギュレーションファイルに保存されます。この情報をデバイスのスタートアップコンフィギュレーションファイルに保存するには、copy running-config startup config 特権 EXEC コマンドを入力します。</p>
mst	(任意) マルチ スパニングツリー (MST) VTP データベース (VTP バージョン 3 に限る) にモードを設定します。
unknown	(任意) 未知の VTP データベース (VTP バージョン 3 に限る) にモードを設定します。
vlan	(任意) VLAN VTP データベースにモードを設定します。これがデフォルトです (VTP バージョン 3 に限る)。
password password	VTP アドバタイズメントで送信され、受信 VTP アドバタイズメントを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメインパスワードを設定します。パスワードは、1 ~ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
hidden	(任意) パスワード文字列から生成されたキーが VLAN データベース ファイルに保存されることを指定します。hidden パスワードを入力した場合、そのパスワードを再入力し、ドメイン内でコマンドを実行する必要があります。このキーワードは、VTP バージョン 3 だけでサポートされています。
secret	(任意) ユーザがパスワードの秘密キーを直接設定できるようにします (VTP バージョン 3 に限る)。
pruning	デバイス上で VTP プルーニングをイネーブルにします。
version number	VTP バージョンをバージョン 1、バージョン 2、またはバージョン 3 に設定します。

Command Default

デフォルトのファイル名は *flash:vlan.dat* です。

デフォルト モードはサーバ モードで、デフォルトのデータベースは VLAN です。

VTP バージョン 3 では、MST データベースのデフォルト モードはトランスペアレントです。

ドメイン名またはパスワードは定義されていません。

パスワードは設定されていません。

プルーニングはディセーブルです。

デフォルトのバージョンはバージョン 1 です。

Command Modes

グローバル コンフィギュレーション

Command History

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines

VTP モード、ドメイン名、および VLAN 設定をデバイスのスタートアップ コンフィギュレーション ファイルに保存して、デバイスを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- スタートアップ コンフィギュレーション および VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され (クリアされ)、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション 内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ~ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

新規データベースをロードするのに **vtp file filename** を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、デバイスは非管理ドメインステートの状態です。非管理ドメインステートの間は、ローカル VLAN 設定に変更が生じて、デバイスは VTP アドバタイズメントを送信しません。デバイスは、トランッキングを行っているポートで最初の VTP サマリー パケットを受信した後、または **vtp domain** コマンドでドメイン名を設定した後で、非管理ドメインステートから抜け出します。装置がサマリー パケットからドメインを受け取る場合は、コンフィギュレーション リビジョン番号が 0 にリセットされます。デバイスが非管理ドメインステートから抜け出したあと、NVRAM をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるとはなりません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、デバイスを VTP サーバモードに戻すことができます。
- **vtp mode server** コマンドは、デバイスがクライアントモードまたはトランスペアレントモードでない場合にエラーを返さないことを除けば、**no vtp mode** と同じです。

- 受信デバイスがクライアントモードである場合、クライアントデバイスはその設定を変更して、サーバの設定をコピーします。クライアントモードのデバイスがある場合には、必ずサーバモードのデバイスですべてのVTPまたはVLAN設定変更を行ってください。サーバモードのデバイスの方が、保持しているVTPコンフィギュレーションリビジョン番号が大きいからです。受信デバイスがトランスペアレントモードである場合、そのデバイスの設定は変更されません。
- トランスペアレントモードのデバイスは、VTPに参加しません。トランスペアレントモードのデバイスでVTPまたはVLAN設定の変更を行った場合、その変更はネットワーク内の他のデバイスには伝播されません。
- サーバモードのデバイスでVTPまたはVLAN設定を変更した場合、その変更は同じVTPドメインのすべてのデバイスに伝播されます。
- **vtp mode transparent** コマンドは、ドメインのVTPをディセーブルにしますが、デバイスからドメインを削除しません。
- VTPバージョン1および2では、VTPおよびVLAN情報を実行コンフィギュレーションファイルに保存する場合には、VTPモードはトランスペアレントに設定してください。
- VTPバージョン1および2では、拡張範囲VLANがスイッチで設定されている場合には、VTPモードをクライアントまたはサーバに変更できません。VTPモードは、VTPバージョン3で拡張VLANを使用することにより変更できます。
- 拡張範囲VLANを追加したり、VTPおよびVLAN情報を実行コンフィギュレーションファイルに保存したりする場合には、VTPモードはトランスペアレントに設定してください。
- ダイナミックVLAN作成がディセーブルの場合、VTPに設定できるモードは、サーバモードまたはクライアントモードのいずれかに限ります。
- **vtp mode off** コマンドを使用すると、デバイスをオフに設定します。**no vtp mode off** コマンドを使用すると、デバイスをVTPサーバモードにリセットします。

VTPパスワードを設定するときには、次の注意事項に従ってください。

- パスワードは大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのデバイスで一致している必要があります。
- デバイスをパスワードが設定されていない状態に戻す場合は、このコマンドの**no vtp password**形式を使用します。
- **hidden** および **secret** キーワードは、VTPバージョン3だけでサポートされています。VTPバージョン2からVTPバージョン3に変換する場合、変換前に**hidden** または **secret** キーワードを削除する必要があります。

VTPプルーニングを設定するときには、次の注意事項に従ってください。

- VTPプルーニングは、プルーニング適格VLANに所属するステーションがない場合、そのVLANの情報をVTP更新から削除します。

- VTP サーバでプルーンングをイネーブルにすると、プルーンングは VLAN ID 1 ~ 1005 の管理ドメイン全体でイネーブルになります。
- プルーンング適格リストに指定された VLAN だけが、プルーンングの対象になります。
- プルーンングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2 (v2) モード ステートを切り替えると、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP デバイスは他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP デバイスでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼働するよう設定する必要があります。
- ドメイン内のすべてのデバイスが VTP バージョン 2 対応である場合、1 つのデバイスでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応デバイスに伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。
- Token Ring Bridge Relay Function (TrBRF) または Token Ring Concentrator Relay Function (TrCRF) VLAN メディア タイプを設定している場合には、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NETVLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。
- VTP バージョン 3 では、VLAN データベース情報だけでなく、すべてのデータベース VTP 情報がその VTP ドメイン全体に伝播します。
- VTP バージョン 3 の 2 つのリージョンが、VTP バージョン 1 または VTP バージョン 2 のリージョン経由で通信できるのは、トランスペアレントモードの場合に限られます。

デバイス コンフィギュレーション ファイルにパスワード、プルーンング、およびバージョン コンフィギュレーションを保存することはできません。

Examples

次の例では、VTP コンフィギュレーション ストレージのファイル名を `vtpfilename` に変更する方法を示します。

```
Device(config)# vtp file vtpfilename
```

次の例では、デバイス ストレージのファイル名をクリアする方法を示します。

```
Device(config)# no vtp file vtpconfig  
Clearing device storage filename.
```

次の例では、このデバイスの VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
Device(config)# vtp interface gigabitethernet
```

次の例では、デバイスの管理ドメインを設定する方法を示します。

```
Device(config)# vtp domain OurDomainName
```

次の例では、デバイスを VTP トランスペアレント モードにする方法を示します。

```
Device(config)# vtp mode transparent
```

次の例では、VTP ドメインパスワードを設定する方法を示します。

```
Device(config)# vtp password ThisIsOurDomainsPassword
```

次の例では、VLAN データベースでのプルーンングをイネーブルにする方法を示します。

```
Device(config)# vtp pruning  
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
Device(config)# vtp version 2
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

vtp (インターフェイス コンフィギュレーション)

ポート単位で VLAN Trunking Protocol (VTP) をイネーブルにするには、インターフェイス コンフィギュレーションモードで **vtp** コマンドを使用します。インターフェイスで VTP をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
vtp
no vtp
```

Syntax Description このコマンドには引数またはキーワードはありません。

Command Modes インターフェイス コンフィギュレーション

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines このコマンドは、トランキング モードのインターフェイスでのみ入力してください。

Examples

次の例では、インターフェイス上で VTP をイネーブルにする方法を示します。

```
Device> enable
Device(config-if)# vtp
```

次の例では、インターフェイス上で VTP をディセーブルにする方法を示します。

```
Device(config-if)# no vtp
```

vtp primary

デバイスを VLAN Trunking Protocol (VTP) プライマリサーバとして設定するには、特権 EXEC モードで **vtp primary** コマンドを使用します。

vtp primary [mst | vlan] [force]

Syntax Description	Parameter	Description
	mst	(任意) デバイスをマルチスパンニングツリー (MST) 機能のプライマリ VTP サーバとして設定します。
	vlan	(任意) デバイスを VLAN のプライマリ VTP サーバとして設定します。
	force	(任意) プライマリサーバを設定するときにデバイスが競合するデバイスをチェックしないように設定します。

Command Default デバイスは VTP セカンダリサーバです。

Command Modes 特権 EXEC

Command History	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

Usage Guidelines VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリサーバは、プライマリサーバから受信したアップデートされた VTP のコンフィギュレーションを NVRAM にバックアップすることができます。

デフォルトでは、すべてのデバイスはセカンダリサーバとして起動します。プライマリサーバのステータスは、管理者がドメイン内のテイクオーバー メッセージを発行する場合のデータベースアップデートのためだけに必要です。プライマリサーバなしで実用 VTP ドメインを持つことができます。

デバイスがリロードするかドメインパラメータが変更された場合、プライマリサーバのステータスは失われます。



Note このコマンドは、デバイスが VTP バージョン 3 を実行している場合にのみサポートされます。

Examples

次の例では、デバイスを VLAN のプライマリ VTP サーバとして設定する方法を示します。

```
Device> enable
Device# vtp primary vlan
```

Setting device to VTP TRANSPARENT mode.

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。