



Catalyst 2960 スイッチ コマンド リファレンス **Catalyst 2960 Switch Command Reference**

Cisco IOS リリース 12.2(50)SE
2009 年 3 月

**【注意】 シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/) をご確認ください。**

**本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、
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。
また、契約等の記述については、弊社販売パートナー、または、
弊社担当者にご確認ください。**

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えられますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任は一切負わないものとします。

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Catalyst 2960 スイッチ コマンド リファレンス

© 2006–2008 Cisco Systems, Inc.

All rights reserved.

Copyright © 2009, シスコシステムズ合同会社.

All rights reserved.



CONTENTS

はじめに	xix
対象読者	xix
目的	xix
表記法	xix
関連資料	xx
マニュアルの入手方法およびテクニカル サポート	xxi

CHAPTER 1

コマンドライン インターフェイス (CLI) の使用	1-1
CLI コマンド モード	1-1
ユーザ EXEC モード	1-3
特権 EXEC モード	1-3
グローバル コンフィギュレーション モード	1-3
インターフェイス コンフィギュレーション モード	1-4
config-vlan モード	1-4
VLAN コンフィギュレーション モード	1-5
ライン コンフィギュレーション モード	1-5

CHAPTER 2

Catalyst 2960 スイッチ Cisco IOS コマンド	2-1
aaa accounting dot1x	2-1
aaa authentication dot1x	2-3
aaa authorization network	2-5
archive download-sw	2-6
archive tar	2-9
archive upload-sw	2-12
arp access-list	2-14
authentication control-direction	2-16
authentication event	2-18
authentication fallback	2-21
authentication host-mode	2-23
authentication open	2-25
authentication order	2-27
authentication periodic	2-29
authentication port-control	2-31

authentication priority	2-33
authentication timer	2-35
authentication violation	2-37
auto qos voip	2-39
boot config-file	2-44
boot enable-break	2-45
boot helper	2-46
boot helper-config-file	2-47
boot manual	2-48
boot private-config-file	2-49
boot system	2-50
channel-group	2-51
channel-protocol	2-55
cisp enable	2-56
class	2-57
class-map	2-59
clear dot1x	2-61
clear eap sessions	2-62
clear energywise neighbors	2-63
clear errdisable interface	2-64
clear arp inspection log	2-65
clear ip arp inspection statistics	2-66
clear ip dhcp snooping	2-67
clear lacp	2-69
clear mac address-table	2-70
clear mac address-table move update	2-72
clear nmsp statistics	2-73
clear pagp	2-74
clear port-security	2-75
clear spanning-tree counters	2-77
clear spanning-tree detected-protocols	2-78
clear vmpls statistics	2-80
clear vtp counters	2-81
cluster commander-address	2-82
cluster discovery hop-count	2-84

cluster enable	2-85
cluster holdtime	2-86
cluster member	2-87
cluster outside-interface	2-89
cluster run	2-90
cluster standby-group	2-91
cluster timer	2-93
define interface-range	2-95
delete	2-97
deny (ARP アクセス リスト コンフィギュレーション)	2-99
deny (MAC アクセス リスト コンフィギュレーション)	2-101
dot1x	2-104
dot1x auth-fail max-attempts	2-106
dot1x auth-fail vlan	2-108
dot1x control-direction	2-110
dot1x credentials (グローバル コンフィギュレーション)	2-112
dot1x critical (グローバル コンフィギュレーション)	2-113
dot1x critical (インターフェイス コンフィギュレーション)	2-115
dot1x default	2-117
dot1x fallback	2-118
dot1x guest-vlan	2-119
dot1x host-mode	2-121
dot1x initialize	2-123
dot1x mac-auth-bypass	2-124
dot1x max-reauth-req	2-126
dot1x max-req	2-127
dot1x pae	2-128
dot1x port-control	2-129
dot1x re-authenticate	2-131
dot1x reauthentication	2-132
dot1x test eapol-capable	2-133
dot1x test timeout	2-134
dot1x timeout	2-135
dot1x violation-mode	2-138
duplex	2-139

energywise (グローバル コンフィギュレーション)	2-141
energywise (インターフェイス コンフィギュレーション)	2-143
energywise domain	2-145
energywise query	2-147
errdisable detect cause	2-151
errdisable detect cause small-frame	2-154
errdisable recovery cause small-frame	2-156
errdisable recovery	2-157
exception crashinfo	2-160
fallback profile	2-161
flowcontrol	2-163
interface port-channel	2-165
interface range	2-167
interface vlan	2-170
ip access-group	2-172
ip address	2-174
ip admission	2-176
ip admission name proxy http	2-178
ip arp inspection filter vlan	2-180
ip arp inspection limit	2-182
ip arp inspection log-buffer	2-184
ip arp inspection trust	2-186
ip arp inspection validate	2-188
ip arp inspection vlan	2-190
ip arp inspection vlan logging	2-191
ip dhcp snooping	2-194
ip dhcp snooping binding	2-195
ip dhcp snooping database	2-197
ip dhcp snooping information option	2-200
ip dhcp snooping information option allow-untrusted	2-202
ip dhcp snooping limit rate	2-204
ip dhcp snooping trust	2-206
ip dhcp snooping verify	2-207
ip dhcp snooping vlan	2-208
ip igmp filter	2-209

ip igmp max-groups	2-211
ip igmp profile	2-213
ip igmp snooping	2-215
ip igmp snooping last-member-query-interval	2-217
ip igmp snooping querier	2-219
ip igmp snooping report-suppression	2-221
ip igmp snooping tcn	2-223
ip igmp snooping tcn flood	2-225
ip igmp snooping vlan immediate-leave	2-226
ip igmp snooping vlan mrouter	2-228
ip igmp snooping vlan static	2-230
ip source binding	2-232
ip ssh	2-234
ip verify source	2-236
ipv6 mld snooping	2-238
ipv6 mld snooping last-listener-query-count	2-240
ipv6 mld snooping last-listener-query-interval	2-242
ipv6 mld snooping listener-message-suppression	2-244
ipv6 mld snooping robustness-variable	2-246
ipv6 mld snooping tcn	2-248
ipv6 mld snooping vlan	2-250
lACP port-priority	2-252
lACP system-priority	2-254
location (グローバル コンフィギュレーション)	2-256
location (インターフェイス コンフィギュレーション)	2-258
link state group	2-260
link state track	2-262
logging event	2-263
logging event power-inline-status	2-264
logging file	2-265
mac access-group	2-267
mac access-list extended	2-269
mac address-table aging-time	2-271
mac address-table learning vlan	2-272
mac address-table move update	2-274

mac address-table notification	2-276
mac address-table static	2-278
mac address-table static drop	2-279
macro apply	2-281
macro auto execute	2-284
macro auto global processing	2-289
macro description	2-291
macro global	2-292
macro global description	2-295
macro name	2-296
match (クラス マップ コンフィギュレーション)	2-298
mdix auto	2-300
media-type	2-301
mls qos	2-303
mls qos aggregate-policer	2-305
mls qos cos	2-307
mls qos dscp-mutation	2-309
mls qos map	2-311
mls qos queue-set output buffers	2-315
mls qos queue-set output threshold	2-317
mls qos rewrite ip dscp	2-319
mls qos srr-queue input bandwidth	2-321
mls qos srr-queue input buffers	2-323
mls qos srr-queue input cos-map	2-325
mls qos srr-queue input dscp-map	2-327
mls qos srr-queue input priority-queue	2-329
mls qos srr-queue input threshold	2-331
mls qos srr-queue output cos-map	2-333
mls qos srr-queue output dscp-map	2-335
mls qos trust	2-337
monitor session	2-339
mvr (グローバル コンフィギュレーション)	2-344
mvr (インターフェイス コンフィギュレーション)	2-347
network-policy	2-350
network-policy profile (グローバル コンフィギュレーション)	2-352

network-policy profile (ネットワーク ポリシー コンフィギュレーション)	2-354
nmsp	2-356
nmsp attachment suppress	2-358
pagp learn-method	2-359
pagp port-priority	2-361
permit (ARP アクセス リスト コンフィギュレーション)	2-363
permit (MAC アクセス リスト コンフィギュレーション)	2-365
police	2-368
police aggregate	2-370
policy-map	2-372
port-channel load-balance	2-374
power inline	2-376
power inline consumption	2-379
power inline police	2-381
priority-queue	2-384
queue-set	2-386
radius-server dead-criteria	2-387
radius-server host	2-389
rcommand	2-391
remote-span	2-393
renew ip dhcp snooping database	2-395
reserved-only	2-397
rmon collection stats	2-399
sdm prefer	2-400
service password-recovery	2-402
service-policy	2-404
set	2-406
setup	2-408
setup express	2-411
shell trigger	2-413
show access-lists	2-415
show archive status	2-418
show arp access-list	2-419
show authentication	2-420
show auto qos	2-424

show boot	2-428
show cable-diagnostics tdr	2-430
show cisp	2-432
show class-map	2-433
show cluster	2-434
show cluster candidates	2-436
show cluster members	2-438
show controllers cpu-interface	2-440
show controllers ethernet-controller	2-442
show controllers power inline	2-449
show controllers tcam	2-451
show controllers utilization	2-453
show dot1x	2-455
show dtp	2-459
show eap	2-461
show energywise	2-464
show env	2-468
show errdisable detect	2-469
show errdisable flap-values	2-471
show errdisable recovery	2-473
show etherchannel	2-475
show fallback profile	2-478
show flowcontrol	2-480
show interfaces	2-482
show interfaces counters	2-491
show inventory	2-494
show ip arp inspection	2-495
show ip dhcp snooping	2-499
show ip dhcp snooping binding	2-500
show ip dhcp snooping database	2-503
show ip dhcp snooping statistics	2-505
show ip igmp profile	2-508
show ip igmp snooping	2-509
show ip igmp snooping groups	2-512
show ip igmp snooping mrouter	2-514

show ip igmp snooping querier	2-516
show ip source binding	2-518
show ip verify source	2-520
show ipv6 mld snooping	2-522
show ipv6 mld snooping address	2-524
show ipv6 mld snooping mrouter	2-526
show ipv6 mld snooping querier	2-528
show ipv6 route updated	2-530
show lacp	2-532
show location	2-536
show link state group	2-539
show mac access-group	2-541
show mac address-table	2-543
show mac address-table address	2-545
show mac address-table aging-time	2-547
show mac address-table count	2-549
show mac address-table dynamic	2-551
show mac address-table interface	2-553
show mac address-table learning	2-555
show mac address-table move update	2-556
show mac address-table notification	2-558
show mac address-table static	2-560
show mac address-table vlan	2-562
show mls qos	2-564
show mls qos aggregate-policer	2-565
show mls qos input-queue	2-566
show mls qos interface	2-568
show mls qos maps	2-572
show mls qos queue-set	2-575
show mls qos vlan	2-577
show monitor	2-578
show mvr	2-581
show mvr interface	2-583
show mvr members	2-585
show network-policy profile	2-587

show nmsp	2-589
show pagp	2-592
show parser macro	2-594
show policy-map	2-597
show port-security	2-599
show power inline	2-602
show sdm prefer	2-606
show setup express	2-608
show shell	2-609
show spanning-tree	2-612
show storm-control	2-618
show system mtu	2-621
show udd	2-623
show version	2-626
show vlan	2-628
show vmps	2-631
show vtp	2-634
shutdown	2-639
shutdown vlan	2-640
small-frame violation rate	2-641
snmp-server enable traps	2-643
snmp-server host	2-647
snmp trap mac-notification	2-652
spanning-tree backbonefast	2-654
spanning-tree bpdudfilter	2-656
spanning-tree bpduguard	2-658
spanning-tree cost	2-660
spanning-tree etherchannel guard misconfig	2-662
spanning-tree extend system-id	2-664
spanning-tree guard	2-666
spanning-tree link-type	2-668
spanning-tree loopguard default	2-670
spanning-tree mode	2-672
spanning-tree mst configuration	2-674
spanning-tree mst cost	2-676

spanning-tree mst forward-time	2-678
spanning-tree mst hello-time	2-679
spanning-tree mst max-age	2-680
spanning-tree mst max-hops	2-682
spanning-tree mst port-priority	2-684
spanning-tree mst pre-standard	2-686
spanning-tree mst priority	2-687
spanning-tree mst root	2-688
spanning-tree port-priority	2-690
spanning-tree portfast (グローバル コンフィギュレーション)	2-692
spanning-tree portfast (インターフェイス コンフィギュレーション)	2-695
spanning-tree transmit hold-count	2-697
spanning-tree uplinkfast	2-698
spanning-tree vlan	2-700
speed	2-703
srr-queue bandwidth limit	2-705
srr-queue bandwidth shape	2-707
srr-queue bandwidth share	2-709
storm-control	2-711
switchport access	2-714
switchport backup interface	2-716
switchport block	2-720
switchport host	2-721
switchport mode	2-722
switchport nonegotiate	2-725
switchport port-security	2-727
switchport port-security aging	2-732
switchport priority extend	2-734
switchport protected	2-736
switchport trunk	2-738
switchport voice vlan	2-741
system mtu	2-743
test cable-diagnostics tdr	2-745
traceroute mac	2-746
traceroute mac ip	2-749

trust	2-751	
udld	2-753	
udld port	2-755	
udld reset	2-757	
vlan (グローバル コンフィギュレーション)		2-758
vlan (VLAN コンフィギュレーション)		2-764
vlan database	2-771	
vmps reconfirm (特権 EXEC)	2-774	
vmps reconfirm (グローバル コンフィギュレーション)		2-775
vmps retry	2-776	
vmps server	2-777	
vtp (グローバル コンフィギュレーション)		2-779
vtp (VLAN コンフィギュレーション)		2-783

APPENDIX A

Catalyst 2960 スイッチ ブートローダ コマンド A-1

boot	A-2
cat	A-4
copy	A-5
delete	A-6
dir	A-7
flash_init	A-9
format	A-10
fsck	A-11
help	A-12
memory	A-13
mkdir	A-14
more	A-15
rename	A-16
reset	A-17
rmdir	A-18
set	A-19
type	A-22
unset	A-23
version	A-25

APPENDIX B**Catalyst 2960 スイッチ デバッグ コマンド B-1**

debug auto qos	B-2
debug backup	B-4
debug cisp	B-5
debug cluster	B-6
debug dot1x	B-8
debug dtp	B-10
debug eap	B-11
debug etherchannel	B-12
debug ilpower	B-14
debug interface	B-15
debug ip dhcp snooping	B-17
debug ip igmp filter	B-18
debug ip igmp max-groups	B-19
debug ip igmp snooping	B-20
debug lacp	B-21
debug lldp packets	B-22
debug mac-notification	B-23
debug matm	B-24
debug matm move update	B-25
debug monitor	B-26
debug mvrdbg	B-28
debug nmsp	B-30
debug nvram	B-31
debug pagp	B-32
debug platform acl	B-33
debug platform backup interface	B-34
debug platform cisp	B-35
debug platform cpu-queues	B-36
debug platform dot1x	B-38
debug platform etherchannel	B-39
debug platform forw-tcam	B-40
debug platform frontend-controller	B-41
debug platform ip arp inspection	B-43
debug platform ip dhcp	B-44

debug platform ip igmp snooping	B-45
debug platform ip source-guard	B-47
debug platform led	B-48
debug platform matm	B-49
debug platform messaging application	B-51
debug platform phy	B-52
debug platform pm	B-54
debug platform port-asic	B-56
debug platform port-security	B-57
debug platform qos-acl-tcam	B-58
debug platform resource-manager	B-59
debug platform snmp	B-60
debug platform span	B-61
debug platform supervisor-asic	B-62
debug platform sw-bridge	B-63
debug platform tcam	B-64
debug platform udld	B-66
debug platform vlan	B-67
debug pm	B-68
debug port-security	B-70
debug qos-manager	B-71
debug spanning-tree	B-72
debug spanning-tree backbonefast	B-74
debug spanning-tree bpdu	B-75
debug spanning-tree bpdu-opt	B-76
debug spanning-tree mstp	B-77
debug spanning-tree switch	B-79
debug spanning-tree uplinkfast	B-81
debug sw-vlan	B-82
debug sw-vlan ifs	B-84
debug sw-vlan notification	B-86
debug sw-vlan vtp	B-87
debug udld	B-89
debug vqpc	B-91

APPENDIX C**Catalyst 2960 スイッチ show platform コマンド C-1**

show platform acl	C-2
show platform backup interface	C-3
show platform etherchannel	C-4
show platform forward	C-5
show platform ip igmp snooping	C-7
show platform layer4op	C-9
show platform mac-address-table	C-10
show platform messaging	C-11
show platform monitor	C-12
show platform mvr table	C-13
show platform pm	C-14
show platform port-asic	C-16
show platform port-security	C-20
show platform qos	C-21
show platform resource-manager	C-22
show platform snmp counters	C-24
show platform spanning-tree	C-25
show platform stp-instance	C-26
stack manager	C-27
show platform tcam	C-28
show platform vlan	C-30

APPENDIX D**オープン ソース ソフトウェアについて D-1**

INDEX



はじめに

対象読者

このマニュアルは、Cisco IOS Command-Line Interface (CLI; コマンドライン インターフェイス) を使用して Catalyst 2960 スイッチ (これ以降、スイッチ) を管理するネットワーキング専門家を対象としています。このマニュアルは、すでに Cisco IOS コマンドおよびスイッチ ソフトウェア機能使用経験があることを前提にしています。また、イーサネットと LAN のコンセプトおよび用語に関してすでに習得済みであることも前提としています。

目的

Catalyst 2960 スイッチでは、Access Control List (ACL; アクセス コントロール リスト) や QoS (Quality of Service) といったエンタープライズクラスのインテリジェントなサービスを提供するソフトウェア イメージをサポートしています。

このマニュアルには、Catalyst 2960 スイッチで使用するために作成または変更されたレイヤ 2 コマンドに必要な情報が記載されています。標準 Cisco IOS Release 12.2 コマンドについては、Cisco.com のホームページにアクセスして ([Technical Support & Documentation] > [Cisco IOS Software])、Cisco IOS のマニュアル セットを参照してください。

このマニュアルでは、お客様のスイッチを設定する手順については説明していません。設定手順については、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。

このマニュアルでは、表示されるシステム メッセージについては説明していません。詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

資料の更新については、このリリースに対応するリリース ノートを参照してください。

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 角カッコ ([]) の中の要素は、省略可能です。

- 必ずどれか 1 つを選択しなければならない要素は、波カッコ ({}) で囲み、縦棒 (|) で区切って示しています。
- 任意で選択する要素の中で、必ずどれか 1 つを選択しなければならない要素は、角カッコと波カッコで囲み、縦棒で区切って ({{|}}) 示しています。

対話形式の例では、次の表記法を使用しています。

- 端末セッションおよびシステムの表示は、screen フォントで示しています。
- ユーザが入力する情報は、**太字の screen** フォントで示しています。
- パスワードやタブのように、出力されない文字は、かぎカッコ (<>) で囲んで示しています。

(注)、注意、および警告には、次の表記法および記号を使用しています。



(注)

「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

以下に挙げる、スイッチに関する詳細情報が記載されているマニュアルは、次の Cisco.com サイトから入手できます。

http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html



(注)

スイッチの取り付け、設定、アップグレードを行う前に、次のマニュアルを参照してください。

- 初期設定情報については、入門ガイドの「Using Express Setup」またはハードウェア インストール ガイドの付録「Configuring the Switch with the CLI-Based Setup Program」を参照してください。
- デバイス マネージャの要件については、リリース ノート（発注できませんが、Cisco.com で入手可能）の「System Requirements」を参照してください。
- Network Assistant の要件については、『Getting Started with Cisco Network Assistant』（発注できませんが、Cisco.com で入手可能）を参照してください。
- クラスタの要件については、『Release Notes for Cisco Network Assistant』（発注できませんが、Cisco.com で入手可能）を参照してください。
- アップグレード情報については、リリース ノートの「Downloading Software」を参照してください。

スイッチに関する他の情報については、次のマニュアルを参照してください。

- 『Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches』
- 『Catalyst 2960 Switch Software Configuration Guide』
- 『Catalyst 2960 Switch Command Reference』
- デバイス マネージャのオンライン ヘルプ（スイッチで利用可能）

- 『*Catalyst 2960 Switch Hardware Installation Guide*』
- 『*Catalyst 2960 Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Catalyst 2960 Switch*』
- 『*Catalyst 3750, 3560, 3550, 2975, 2970, and 2960 Switch System Message Guide*』
- 『*Getting Started with Cisco Network Assistant*』
- 『*Release Notes for Cisco Network Assistant*』
- 『*Cisco Small Form-Factor Pluggable Modules Installation Notes*』
- 『*Cisco CWDM GBIC and CWDM SFP Modules Installation Note*』
- 『*Cisco RPS 300 Redundant Power System Hardware Installation Guide*』
- 『*Cisco RPS 675 Redundant Power System Hardware Installation Guide*』
- 『*Cisco Redundant Power System 2300 Hardware Installation Guide*』 (Customer Order Number DOC-7817647=)
- Network Admission Control (NAC) 機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- これらの互換性マトリクス ドキュメントは、Cisco.com の次のページで入手可能です。
http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html
 - 『*Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*』
 - 『*Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*』
 - 『*Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*』
 - 『*Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



CHAPTER 1

コマンドライン インターフェイス (CLI) の使用

Catalyst 2960 スイッチは Cisco IOS ソフトウェアによってサポートされています。ここでは、ソフトウェア機能を設定するためのスイッチ Command-Line Interface (CLI; コマンドライン インターフェイス) の使用方法について説明します。

- これらの機能をサポートするコマンドの詳細については、第 2 章「[Catalyst 2960 スイッチ Cisco IOS コマンド](#)」を参照してください。
- ブートローダ コマンドの詳細については、[付録 A「Catalyst 2960 スイッチ ブートローダ コマンド](#)」を参照してください。
- **debug** コマンドの詳細については、[付録 B「Catalyst 2960 スイッチ デバッグ コマンド](#)」を参照してください。
- **show platform** コマンドの詳細については、[付録 C「Catalyst 2960 スイッチ show platform コマンド](#)」を参照してください。
- Cisco IOS Release 12.2 のさらに詳しい情報については、『*Cisco IOS Release 12.2 Command Summary*』を参照してください。
- タスク指向の設定手順については、このリリースのソフトウェア コンフィギュレーション ガイドを参照してください。

このマニュアルでは、IP Version 6 (IPv6) に関して特に記載がない限り、IP は IP Version 4 (IPv4) を指します。

CLI コマンド モード

ここでは、CLI コマンド モード構造について説明します。コマンド モードは、特定の Cisco IOS コマンドをサポートします。たとえば、**interface interface-id** コマンドは、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ときだけ機能します。

以下は、スイッチの主なコマンド モードです。

- ユーザ EXEC
- 特権 EXEC
- グローバル コンフィギュレーション
- インターフェイス コンフィギュレーション
- config-vlan
- VLAN コンフィギュレーション

CLI コマンド モード

- ライン コンフィギュレーション

表 1-1 に、主なコマンドモード、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。表示されているプロンプトは、デフォルト名 *Switch* を使用しています。

表 1-1 コマンドモードの概要

コマンドモード	アクセス方法	プロンプト	終了または次のモードのアクセス
ユーザ EXEC	これが最初のアクセス レベルです。 (スイッチについては) ターミナル設定を変更し、基本タスクを実行し、システム情報を一覧表示します。	Switch>	logout コマンドを入力します。 特権 EXEC モードを開始するには、 enable コマンドを入力します。
特権 EXEC	ユーザ EXEC モードから、 enable コマンドを入力します。	Switch#	ユーザ EXEC モードに戻る場合は、 disable コマンドを入力します。 グローバル コンフィギュレーション モードを開始するには、 configure コマンドを入力します。
グローバル コンフィギュレーション	特権 EXEC モードから、 configure コマンドを入力します。	Switch(config)#	特権 EXEC モードに戻る場合は、 exit または end コマンドを入力するか、 Ctrl-Z を押します。 インターフェイス コンフィギュレーション モードを開始するには、 interface コンフィギュレーション コマンドを入力します。
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 モードから、 interface コマンドを入力し、次にインターフェイス ID を入力することにより、インターフェイスを指定します。	Switch(config-if)#	特権 EXEC モードに戻る場合は、 end コマンドを入力するか、 Ctrl-Z を押します。 グローバル コンフィギュレーション モードに戻る場合は、 exit コマンドを入力します。
config-vlan	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。	Switch(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 モードに戻る場合は、 end コマンドを入力するか、 Ctrl-Z を押します。
VLAN コンフィギュレーション	特権 EXEC モードから、 vlan database コマンドを入力します。	Switch(vlan)#	特権 EXEC モードに戻る場合は、 exit コマンドを入力します。
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 モードから、 line コマンドを入力することにより、ラインを指定します。	Switch(config-line)#	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 モードに戻る場合は、 end コマンドを入力するか、 Ctrl-Z を押します。

ユーザ EXEC モード

装置にアクセスすると、自動的にユーザ EXEC コマンド モードに入ります。ユーザ レベルで使用可能な EXEC コマンドは、特権レベルで使用可能な EXEC コマンドのサブセットです。一般に、ユーザ EXEC コマンドは、端末設定の一時的変更、基本テストの実行、システム情報の一覧表示などに使用します。

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符 (?) を入力します。

```
Switch> ?
```

特権 EXEC モード

特権コマンドの多くは動作パラメータの設定に関係しています。無許可の使用を防止するには、特権コマンドへのアクセスをパスワードで保護する必要があります。特権コマンドセットには、ユーザ EXEC モードのコマンドと、それ以外のコマンド モードにアクセスするための **configure** 特権 EXEC コマンドが含まれます。

システム管理者がパスワードを設定した場合、特権 EXEC モードへのアクセスが許可される前に、パスワードの入力を要求するプロンプトが表示されます。パスワードは画面には表示されません。また、大文字と小文字が区別されます。

特権 EXEC モードのプロンプトは、装置名のあとにポンド記号 (#) が付きます。

```
Switch#
```

特権 EXEC モードにアクセスするには、**enable** コマンドを入力します。

```
Switch> enable  
Switch#
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符 (?) を入力します。

```
Switch# ?
```

ユーザ EXEC モードに戻る場合は、**disable** 特権 EXEC コマンドを入力します。

グローバル コンフィギュレーション モード

グローバル コンフィギュレーション コマンドは、装置全体に影響を与える機能に適用されます。グローバル コンフィギュレーション モードを開始するには、**configure** 特権 EXEC コマンドを使用します。デフォルトでは、管理コンソールからコマンドを入力します。

configure コマンドを入力すると、コンフィギュレーション コマンドの送信元の入力を要求するメッセージが表示されます。

```
Switch# configure  
Configuring from terminal, memory, or network [terminal]?
```

コンフィギュレーション コマンドの送信元として、端末または NVRAM (不揮発性 RAM) のいずれかを指定することができます。

次の例では、グローバル コンフィギュレーション モードにアクセスする方法を示します。

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符 (?) を入力します。

```
Switch(config)# ?
```

グローバル コンフィギュレーション コマンド モードを終了して特権 EXEC モードに戻る場合は、**end** コマンドまたは **exit** コマンドを入力するか、**Ctrl-Z** を押します。

インターフェイス コンフィギュレーション モード

インターフェイス コンフィギュレーション コマンドは、インターフェイスの動作を変更します。インターフェイス コンフィギュレーション コマンドは常に、インターフェイス タイプを定義するグローバル コンフィギュレーション コマンドのあとに続きます。

インターフェイス コンフィギュレーション モードにアクセスするには、**interface interface-id** コマンドを使用します。次の新しいプロンプトはインターフェイス コンフィギュレーション モードを示しています。

```
Switch(config-if)#
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符 (?) を入力します。

```
Switch(config-if)# ?
```

インターフェイス 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 モードに戻る場合は、**exit** コマンドを入力します。インターフェイス コンフィギュレーション モードを終了して特権 EXEC モードに戻る場合は、**end** コマンドを入力するか、**Ctrl-Z** を押します。

config-vlan モード

標準範囲 VLAN (仮想 LAN) (VLAN ID 1 ~ 1005) を設定したり、VTP モードがトランスペアレントであるときに拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を設定したりする場合は、このモードを使用します。VTP モードが透過型である場合は、VLAN および VTP 設定は実行コンフィギュレーション ファイルに保存されるので、**copy running-config startup-config** 特権 EXEC コマンドを実行して、この設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存できます。VTP が透過モードまたはサーバモードの場合、VLAN ID が 1 ~ 1005 の VLAN 設定は、VLAN データベースに保存されます。拡張範囲 VLAN 設定は、VLAN データベースには保存されません。

config-vlan モードを開始するには、**vlan vlan-id** グローバル コンフィギュレーション コマンドを入力します。

```
Switch(config)# vlan 2000  
Switch(config-vlan)#
```

サポートされるキーワードはさまざまですが、VLAN コンフィギュレーション モードで利用できるコマンドと似ています。コマンドの包括的なリストを表示するには、プロンプトで疑問符 (?) を入力します。

```
Switch(config-vlan)# ?
```

拡張範囲 VLAN については、MTU サイズ以外のすべての特性はデフォルト設定のままにしておいてください。

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** を入力します。特権 EXEC モードに戻る場合は、**end** を入力します。**shutdown** 以外のすべてのコマンドは、**config-vlan** モードを終了したときに有効になります。

VLAN コンフィギュレーション モード

VLAN コンフィギュレーション コマンドを使用すると、VLAN ID 1 ~ 1005 の VLAN パラメータを作成または変更することができます。

VLAN コンフィギュレーション モードにアクセスするには、**vlan database** 特権 EXEC コマンドを入力します。

```
Switch# vlan database  
Switch(vlan)#
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符 (?) を入力します。

```
Switch(vlan)# ?
```

特権 EXEC モードに戻る場合は、**abort** VLAN コンフィギュレーション コマンドを入力して、設定予定だったデータベースを放棄します。または、**exit** を入力して、設定対象の新しい VLAN データベースを実装し、特権 EXEC モードに戻ります。**exit** または **apply** を入力した場合、設定が VLAN データベースに保存され、VLAN コンフィギュレーション モードからの設定はスイッチ コンフィギュレーション ファイルに保存することはできません。

ライン コンフィギュレーション モード

ライン コンフィギュレーション コマンドは、端末ラインの動作を変更します。ライン コンフィギュレーション コマンドは、常にライン番号を定義するライン コマンドのあとに来ます。端末パラメータ設定をラインごと、あるいはある範囲のライン全体で変更するには、このコマンドを使用します。

ライン コンフィギュレーション モードを開始するには、**line vty line_number [ending_line_number]** コマンドを使用します。次の新しいプロンプトはライン コンフィギュレーション モードを示しています。次の例では、仮想端末ライン 7 でライン コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# line vty 0 7
```

サポートされているコマンドは、ご使用のソフトウェアのバージョンによって異なります。コマンドの包括的なリストを表示するには、プロンプトで疑問符 (?) を入力します。

```
Switch(config-line)# ?
```

ライン 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 モードに戻る場合は、**exit** コマンドを使用します。ライン コンフィギュレーション モードを終了して特権 EXEC モードに戻る場合は、**end** コマンドを入力するか、**Ctrl-Z** を押します。



CHAPTER 2

Catalyst 2960 スイッチ Cisco IOS コマンド

aaa accounting dot1x

Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントティング) アカウントティングをイネーブルにし、回線単位またはインターフェイス単位で IEEE 802.1x セッションに対して特定のアカウントティング方式を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場合は、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}
```

シンタックスの説明

name	サーバグループ名。これは、 broadcast group および group キーワードのあとに入力する場合のオプションです。
default	アカウントティング サービスのデフォルトのリストとしてあとに続くアカウントティング方式を使用します。
start-stop	プロセスの最初にアカウントティング開始通知を送信し、プロセスの終了時にアカウントティング終了通知を送信します。アカウントティング開始レコードは、バックグラウンドで送信されます。アカウントティング開始通知がアカウントティング サーバで受信されたかどうかにかかわらず、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバへのアカウントティング レコードの送信をイネーブルにし、各グループの最初のサーバにアカウントティング レコードを送信します。最初のサーバが使用不可の場合、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 : サーバグループ名• radius : 全 RADIUS ホストのリスト• tacacs+ : 全 TACACS+ ホストのリスト group キーワードは、 broadcast group および group キーワードのあとに入力する場合のオプションです。複数のオプション group キーワードを入力できます。

aaa accounting dot1x

radius	(任意) RADIUS 認証をイネーブルにします。
tacacs+	(任意) TACACS+ アカウンティングをイネーブルにします。

デフォルト

AAA アカウンティングはディセーブルです。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、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。

例

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。

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting dot1x default start-stop group radius
```



(注)

RADIUS 認証サーバは、AAA クライアントからの更新またはウォッチドッグ パケットを受け入れてロギングするように、適切に設定されている必要があります。

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1x が動作しているインターフェイスで使用する 1 つまたは複数の AAA を指定します。
aaa new-model	AAA アクセス制御モデルをイネーブルにします。構文情報については、「Cisco IOS Security Command Reference, Release 12.2」 > 「Authentication, Authorization, and Accounting」 > 「Authentication Commands」を参照してください。
dot1x reauthentication	定期的な再認証をイネーブルまたはディセーブルにします。
dot1x timeout reauth-period	再認証の間隔 (秒) を指定します。

aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで使用する認証、認可、アカウントリング (AAA) 方式を指定するには、**aaa authentication 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。認証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。

```
aaa authentication dot1x {default} method1
```

```
no aaa authentication dot1x {default}
```

シンタックスの説明

default	この引数に続ける認証方式をログイン時のデフォルトの方式として使用します。
method1	認証用にすべての RADIUS サーバのリストを使用するには、 group radius キーワードを入力します。



(注)

他のキーワードがコマンドラインのヘルプ スtring に表示されますが、サポートされているのは **default** および **group radius** キーワードだけです。

デフォルト

認証は実行されません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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一定の順序で試みる方式を指定します。実際に 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。

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 コマンドを使用して RADIUS サーバを設定する必要があります。

設定された認証方式のリストを表示する場合は、**show running-config** 特権 EXEC コマンドを使用します。

例

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 サーバとの通信を試行します。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。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

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。

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス制御モデルをイネーブルにします。構文情報については、「Cisco IOS Security Command Reference, Release 12.2」>「Authentication, Authorization, and Accounting」>「Authentication Commands」を参照してください。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

aaa authorization network

IEEE 802.1x Virtual LAN (VLAN; 仮想 LAN) 割り当てなどのすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を使用するようにスイッチを設定するには、**aaa authorization network** 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。RADIUS ユーザ認証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。

aaa authorization network default group radius

no aaa authorization network default

シンタックスの説明

default group radius	デフォルトの認証リストとして、サーバ グループ内のすべての RADIUS ホストのリストを使用します。
-----------------------------	---

デフォルト

認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが、デフォルトの認証リスト内にある RADIUS サーバから IEEE 802.1x 認証パラメータをダウンロードできるようにするには、**aaa authorization network default group radius** 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。認証パラメータは、VLAN 割り当てなど、RADIUS サーバからパラメータを取得する機能で使用されます。

設定された認証方式リストを表示する場合は、**show running-config** 特権 EXEC コマンドを使用します。

例

この例では、すべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を行うようスイッチを設定する方法を示します。

```
Switch(config)# aaa authorization network default group radius
```

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。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

archive download-sw

新しいイメージを TFTP サーバからスイッチにダウンロードし、既存のイメージを上書きまたは保持するには、**archive download-sw** 特権 EXEC コマンドを使用します。

```
archive download-sw {/directory | /force-reload | /imageonly | /leave-old-sw |
/no-set-boot | no-version-check | /overwrite | /reload | /safe} source-url
```

シンタックスの説明

/directory	イメージのディレクトリを指定します。
/force-reload	ソフトウェア イメージのダウンロードが成功したあと、無条件にシステムのリロードを強制します。
/imageonly	ソフトウェア イメージだけをダウンロードし、組み込みデバイス マネージャに関連する HTML ファイルはダウンロードしません。既存のバージョンの HTML ファイルは、既存のバージョンが上書きまたは削除されている場合にだけ削除されます。
/leave-old-sw	ダウンロードが成功したあと、古いソフトウェア バージョンを保存します。
/no-set-boot	新しいソフトウェア イメージのダウンロードが成功したあと、BOOT 環境変数の設定は新しいソフトウェア イメージをポイントするように変更されません。
/no-version-check	スイッチで稼働中のイメージとの互換性を持つバージョンであるかどうかを確認せずに、ソフトウェア イメージをダウンロードします。
/overwrite	ダウンロードされたソフトウェア イメージで、フラッシュ メモリのソフトウェア イメージを上書きします。
/reload	変更された設定が保存されていない場合を除き、イメージのダウンロードに成功したあとでシステムをリロードします。
/safe	現在のソフトウェア イメージを維持します。新しいイメージがダウンロードされるまでは、新しいソフトウェア イメージ用の領域を作る目的で現在のソフトウェア イメージを削除しません。ダウンロード終了後に現在のイメージが削除されます。

<i>source-url</i>	<p>ローカル ファイル システムまたはネットワーク ファイル システム用の送信元 URL エイリアス。次のオプションがサポートされています。</p> <ul style="list-style-type: none"> 2 番目のブートローダ (BS1) の構文 bs1: ローカル フラッシュ ファイル システムの構文 flash: FTP の構文 ftp:[[/username[:password]@location]/directory]/image-name.tar HTTP サーバの構文 http://[[username:password]@]{hostname host-ip}/[directory]/image-name.tar セキュア HTTP サーバの構文 https://[[username:password]@]{hostname host-ip}/[directory]/image-name.tar Remote Copy Protocol (RCP) の構文 rcp:[[/username@location]/directory]/image-name.tar TFTP の構文 tftp:[[/location]/directory]/image-name.tar <p><i>image-name.tar</i> は、スイッチにダウンロードし、インストールするソフトウェア イメージです。</p>
-------------------	--

デフォルト

現行のソフトウェア イメージは、ダウンロードされたイメージで上書きされません。

ソフトウェア イメージと HTML ファイルの両方がダウンロードされます。

新しいイメージは **flash:** ファイル システムにダウンロードされます。

flash: ファイル システムの新しいソフトウェア イメージを指定するように BOOT 環境変数が変更されます。

イメージ名では大文字と小文字が区別されます。イメージ ファイルは **tar** フォーマットで提供されます。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

/imageonly オプションは、既存のイメージが削除または置き換えられている場合に、既存のイメージの HTML ファイルを削除します。(HTML ファイルのない) Cisco IOS イメージだけがダウンロードされます。

/safe または **/leave-old-sw** オプションを使用した場合に、十分なフラッシュ メモリがないと、新しいイメージのダウンロードに失敗する場合があります。ソフトウェアを残すことによってフラッシュ メモリの空き容量が不足し、新しいイメージが入りきらなかった場合に、エラーが発生します。

/leave-old-sw オプションを使用したために、新しいイメージをダウンロードしても古いイメージを上書きしなかった場合、**delete** 特権 EXEC コマンドを使用して古いイメージを削除することができます。詳細については、P.2-97 の「**delete**」を参照してください。

フラッシュ デバイスのイメージを、ダウンロードされたイメージで上書きする場合は、**/overwrite** オプションを使用します。

/overwrite オプションなしでこのコマンドを指定する場合、ダウンロードアルゴリズムは、新しいイメージが、スイッチ フラッシュ デバイスのイメージと同じではないことを確認します。イメージが同じである場合には、ダウンロードは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがダウンロードされます。

新しいイメージをダウンロードしたあとで、**reload** 特権 EXEC コマンドを入力して新しいイメージの使用を開始するか、**archive download-sw** コマンドの **/reload** または **/force-reload** オプションを指定してください。

例

次の例では、172.20.129.10 の TFTP サーバから新しいイメージをダウンロードし、スイッチでイメージを上書きする方法を示します。

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

次の例では、172.20.129.10 の TFTP サーバからソフトウェア イメージだけをスイッチにダウンロードする方法を示します。

```
Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

次の例では、ダウンロードが成功したあとで古いソフトウェア バージョンを保存する方法を示します。

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

関連コマンド

コマンド	説明
archive tar	tar ファイルの作成、tar ファイル内のファイルを一覧表示、tar ファイルからのファイル抽出を行います。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。
delete	フラッシュ メモリ デバイスのファイルまたはディレクトリを削除します。

archive tar

tar ファイルの作成、tar ファイル内のファイルの一覧表示、tar ファイルからのファイル抽出を実行するには、**archive tar** 特権 EXEC コマンドを使用します。

```
archive tar {/create destination-url flash:/file-url} | {/table source-url} | {/xtract source-url flash:/file-url [dir/file...]}
```

シンタックスの説明

/create destination-url
flash:/file-url

ローカル ファイル システムまたはネットワーク ファイル システムに新しい tar ファイルを作成します。

destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL エイリアスおよび作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの構文
flash:
- FTP の構文
ftp:[[/username[:password]@location]/directory]/tar-filename.tar
- HTTP サーバの構文
http://[[username:password]@]{hostname | host-ip}[/directory]/image-name.tar
- セキュア HTTP サーバの構文
https://[[username:password]@]{hostname | host-ip}[/directory]/image-name.tar
- Remote Copy Protocol (RCP) の構文
rep:[[/username@location]/directory]/tar-filename.tar
- TFTP の構文 **tftp:[[/location]/directory]/tar-filename.tar**

tar-filename.tar は、作成する tar ファイルです。

flash:/file-url には、新しい tar ファイルが作成されるローカル フラッシュ ファイル システムの場所を指定します。

送信元ディレクトリ内のファイルまたはディレクトリのオプションのリストを指定して、新しい tar ファイルに書き込むことができます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

/table source-url	<p>既存の tar ファイルの内容を画面に表示します。</p> <p><i>source-url</i> には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。</p> <ul style="list-style-type: none"> ローカル フラッシュ ファイル システムの構文 flash: FTP の構文 ftp:[[/username[:password]@location]/directory]/tar-filename.tar HTTP サーバの構文 http://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar セキュア HTTP サーバの構文 https://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar RCP の構文 rnp:[[/username@location]/directory]/tar-filename.tar TFTP の構文 tftp:[[/location]/directory]/tar-filename.tar <p><i>tar-filename.tar</i> は、表示する tar ファイルです。</p>
/xtract source-url flash:/file-url [dir/file...]	<p>tar ファイルからローカル ファイル システムにファイルを抽出します。</p> <p><i>source-url</i> には、ローカル ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。</p> <ul style="list-style-type: none"> ローカル フラッシュ ファイル システムの構文 flash: FTP の構文 ftp:[[/username[:password]@location]/directory]/tar-filename.tar HTTP サーバの構文 http://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar セキュア HTTP サーバの構文 https://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar RCP の構文 rnp:[[/username@location]/directory]/tar-filename.tar TFTP の構文 tftp:[[/location]/directory]/tar-filename.tar <p><i>tar-filename.tar</i> は、抽出が行われる tar ファイルです。</p> <p>flash:/file-url [dir/file...] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、<i>dir/file...</i> オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。</p>

デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
イメージ名では、大文字と小文字が区別されます。

例

次の例では、tar ファイルを作成する方法を示します。このコマンドはローカル フラッシュ デバイスの *new-configs* ディレクトリの内容を、172.20.10.30 の TFTP サーバの *saved.tar* という名前のファイルに書き込みます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new_configs
```

次の例では、フラッシュ メモリ内のファイルの内容を表示する方法を示します。tar ファイルの内容が画面に表示されます。

```
Switch# archive tar /table flash:c2960-lanbase-tar.12-25.FX.tar
info (219 bytes)
```

```
c2960-lanbase-mz.12-25.FX/ (directory)
c2960-lanbase-mz.12-25.FX (610856 bytes)
c2960-lanbase-mz.12-25.FX/info (219 bytes)
info.ver (219 bytes)
```

次の例では、/html ディレクトリおよびその内容だけを表示する方法を示します。

```
Switch# archive tar /table flash:c2960-lanbase-12-25.FX.tar c2960-lanbase-12-25/html
c2960-lanbase-mz.12-25.FX/html/ (directory)
c2960-lanbase-mz.12-25.FX/html/const.htm (556 bytes)
c2960-lanbase-mz.12-25.FX/html/xhome.htm (9373 bytes)
c2960-lanbase-mz.12-25.FX/html/menu.css (1654 bytes)
<output truncated>
```

次の例では、172.20.10.30 の TFTP サーバの tar ファイルの内容を抽出する方法を示します。ここでは、ローカル フラッシュ ファイル システムのルート ディレクトリに単に *new-configs* ディレクトリを抽出しています。*saved.tar* ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

関連コマンド

コマンド	説明
archive download-sw	TFTP サーバからスイッチに新しいイメージをダウンロードします。
archive upload-sw	スイッチの既存のイメージをサーバにアップロードします。

archive upload-sw

スイッチの既存のイメージをサーバにアップロードするには、**archive upload-sw** 特権 EXEC コマンドを使用します。

archive upload-sw [/version *version_string*] **destination-url**

シンタックスの説明

/version <i>version_string</i>	(任意) アップロードするイメージの特定バージョン文字列を指定します。
destination-url	ローカル ファイル システムまたはネットワーク ファイル システムの宛先 URL エイリアス。次のオプションがサポートされています。 <ul style="list-style-type: none"> ローカル フラッシュ ファイル システムの構文 flash: FTP の構文 ftp:[[/username[:password]@]location]/directory/image-name.tar HTTP サーバの構文 http://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar セキュア HTTP サーバの構文 https://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar Secure Copy Protocol (SCP) の構文 scp:[[/username@]location]/directory/image-name.tar Remote Copy Protocol (RCP) の構文 rcp:[[/username@]location]/directory/image-name.tar TFTP の構文 tftp:[[/location]/directory]/image-name.tar <p><i>image-name.tar</i> は、サーバに保存するソフトウェア イメージの名前です。</p>

デフォルト

フラッシュ ファイル システムから現在稼動中のイメージをアップロードします。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

組み込みデバイス マネージャに関連付けられている HTML ファイルが既存のイメージとともにインストールされている場合にだけ、アップロード機能を使用します。

これらのファイルは、Cisco IOS イメージ、HTML ファイル、info の順序でアップロードされます。これらのファイルがアップロードされると、ソフトウェアは tar ファイルを作成します。

イメージ名では、大文字と小文字が区別されます。

例 次の例では、現在実行中のイメージを、172.20.140.2 の TFTP サーバへアップロードする方法を示します。

```
Switch# archive upload-sw tftp://172.20.140.2/test-image.tar
```

関連コマンド

コマンド	説明
archive download-sw	新しいイメージをスイッチにダウンロードします。
archive tar	tar ファイルの作成、tar ファイル内のファイルを一覧表示、tar ファイルからのファイル抽出を行います。

arp access-list

Address Resolution Protocol (ARP; アドレス解決プロトコル) Access Control List (ACL; アクセスコントロールリスト) を定義したり、すでに定義済みのリストの末尾に句を追加したりするには、**arp access-list** 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 ARP アクセスリストを削除する場合は、このコマンドの **no** 形式を使用します。

arp access-list *acl-name*

no arp access-list *acl-name*

シンタックスの説明

<i>acl-name</i>	ACL の名前です。
-----------------	------------

デフォルト

ARP アクセス リストが定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

arp access-list コマンドを入力すると、ARP アクセス リスト コンフィギュレーション モードが開始され、これら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。

- **default** : コマンドをデフォルト設定に戻します。
- **deny** : 拒否するパケットを指定します。詳細については、[P.2-99 の「deny \(ARP アクセス リスト コンフィギュレーション\)」](#)を参照してください。
- **exit** : ARP アクセス リスト 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か、またはデフォルト設定に戻します。
- **permit** : 転送するパケットを指定します。詳細については、[P.2-363 の「permit \(ARP アクセス リスト コンフィギュレーション\)」](#)を参照してください。

指定した照合条件に基づいて ARP パケットを転送および廃棄するには、**permit** および **deny** アクセス リスト コンフィギュレーション コマンドを使用します。

ARP ACL を定義したら、**ip arp inspection filter vlan** 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その ACL を VLAN に適用できます。IP-to-MAC アドレス バインディングを含む ARP パケットだけが ACL と比較されます。それ以外のタイプのパケットはすべて検証なしで入力 VLAN でブリッジングされます。パケットが ACL で許可されると、スイッチはそのパケットを転送します。明示的な **deny** 文によってパケットが ACL で拒否されると、スイッチはそのパケットを廃棄します。暗黙的な **deny** 文によってパケットが ACL で拒否されると、スイッチはそのパケットを DHCP バインディングのリストと比較します (ただし、ACL がスタティックの場合を除きます。この場合は、パケットがバインディングと比較されません)。

例 次の例では、ARP アクセスリストを定義し、IP アドレス 1.1.1.1 および MAC アドレス 0000.0000.abcd のホストからの ARP 要求と ARP 応答をいずれも許可する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 00001.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny (ARP アクセスリスト コンフィギュレーション)	DHCP バインディングと比較して一致した ARP パケットを拒否します。
ip arp inspection filter vlan	スタティック IP アドレスが設定されたホストからの ARP 要求と ARP 応答を許可します。
permit (ARP アクセスリスト コンフィギュレーション)	DHCP バインディングと比較して一致した ARP パケットを許可します。
show arp access-list	ARP アクセスリストの詳細を表示します。

authentication control-direction

ポートを単一方向モードまたは双方向モードに設定するには、**authentication control-direction** 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。

authentication control-direction {both | in}

no authentication control-direction

シンタックスの説明

both	ポートの双方向制御をイネーブルにします。ポートは、ホストにパケットを送受信できません。
in	ポートの単一方向制御をイネーブルにします。ポートは、ホストにパケットを送信できますが、受信はできません。

デフォルト

ポートは双方向モードに設定されています。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

デフォルト設定（双方向モード）に戻すには、このコマンドの **both** キーワードまたは **no** 形式を使用します。

例

次の例では、双方向モードをイネーブルにする方法を示します。

```
Switch(config)# authentication control-direction both
```

次の例では、単一方向モードをイネーブルにする方法を示します。

```
Switch(config)# authentication control-direction in
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication event	特定の認証イベントに対するアクションを設定します。
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン 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	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上で再認証をイネーブ爾またはディセーブ爾にします。
authentication port-control	ポートの許可ステートの手動制御をイネーブ爾にします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication event

ポート上の特定の認証イベントに対するアクションを設定するには、**authentication event** 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。

```
authentication event fail {[action [authorize vlan vlan-id | next-method] [| retry {retry
count}] } { no-response action authorize vlan vlan-id} {server {alive action
reinitialize} | {dead action authorize}}
```

```
no authentication event fail {[action[authorize vlan vlan-id | next-method] [| retry
{retry count}] } {no-response action authorize vlan vlan-id} {server {alive action
reinitialize} | {dead action authorize}}
```

シンタックスの説明

action	認証イベントに必要なアクションを設定します。
alive	活動状態の認証、認可、アカウントिंग (AAA) サーバに対するアクションを設定します。
authorize	ポートを許可します。
dead	停止状態の AAA サーバに対するアクションを設定します。
fail	failed-authentication パラメータを設定します。
next-method	次の認証方式に移行します。
no-response	応答のないホストに対するアクションを設定します。
reinitialize	許可されたすべてのクライアントを再初期化します。
retry	認証に失敗したあとの再試行をイネーブルにします。
<i>retry count</i>	再試行回数 (0 ~ 5 回) を設定します。
server	AAA サーバ イベントに対するアクションを設定します。
vlan	authentication-fail VLAN を指定します (1 ~ 4094)。
<i>vlan-id</i>	VLAN の ID 番号を指定します (1 ~ 4094)。

デフォルト

ポート上でイベント応答が設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

特定のアクションに対するスイッチの応答を設定するには、このコマンドに **fail**、**no-response**、または **event** キーワードを指定します。

server-dead イベントの場合：

- スイッチが **critical-authentication** ステートに移行すると、認証中の新しいホストだけが **critical-authentication** VLAN に移行します。認証済のホストは認証済の VLAN にそのまま残り、再認証タイマーがディセーブルになります。

- クライアントで Windows XP が稼動しており、クライアントの接続先のクリティカル ポートが `critical-authentication` ステートの場合は、インターフェイスが認証されていないことが Windows XP から通知されることがあります。

Windows XP クライアントが DHCP に設定されており、DHCP サーバから IP アドレスが割り当てられていると、クリティカル ポートが EAP 認証成功メッセージを受信しても、DHCP 設定プロセスで再初期化が実行されない場合があります。

no-response イベントの場合：

- IEEE 802.1x ポート上でゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN (EAPOL) Request/Identity フレームに対する応答を受信しないか、または EAPOL パケットがクライアントから送信されないと、スイッチはクライアントをゲスト VLAN に割り当てます。
- スイッチは、EAPOL パケット履歴を保持します。リンクの有効期間中に別の EAPOL パケットがポート上で検出されると、ゲスト VLAN 機能がディセーブルになります。ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。EAPOL 履歴がクリアされます。
- スイッチ ポートがゲスト VLAN (複数ホスト モード) に移行すると、複数の IEEE 802.1x 非対応クライアントへのアクセスが許可されます。ゲスト VLAN が設定されているポートに IEEE 802.1x 対応クライアントが加入すると、そのポートが RADIUS 設定 VLAN またはユーザ設定アクセス VLAN で無許可ステートに移行し、認証が再開されます。

Remote Switched Port Analyzer (RSPAN; リモート スイッチド ポート アナライザ) VLAN、プライマリ プライベート VLAN、音声 VLAN 以外のアクティブな VLAN をすべて、IEEE 802.1x のゲスト VLAN として設定できます。ゲスト VLAN の機能は、アクセス ポートでのみサポートされています。内部 VLAN (ルーテッド ポート) とトランク ポートではサポートされていません。

- MAC 認証バイパスが IEEE 802.1x ポートでイネーブルになっている場合、EAPOL メッセージ交換の待機中に IEEE802.1x 認証が期限切れになると、スイッチはクライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。
 - 認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。
 - 認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます (指定されていない場合)。

詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with MAC Authentication Bypass」を参照してください。

authentication-fail イベントの場合：

- サブリカントが認証に失敗すると、ポートが制限 VLAN に移行し、EAP 認証成功メッセージがサブリカントに送信されます。これは、サブリカントに実際の認証失敗が通知されないためです。
 - EAP の成功メッセージが送信されない場合、サブリカントは 60 秒ごと (デフォルト) に EAP 開始メッセージを送信して認証を行おうとします。
 - 一部のホスト (たとえば、Windows XP を実行中のデバイス) は、EAP の成功メッセージを受け取るまで Dynamic Host Configuration Protocol (DHCP) を実行できません。

制限 VLAN は、シングルホスト モード (デフォルトのポート モード) でのみサポートされます。ポートが制限 VLAN に配置されると、サブリカントの MAC アドレスが MAC アドレス テーブルに追加されます。ポート上のその他の MAC アドレスはセキュリティ違反として扱われます。

- レイヤ 3 ポート用の内部 VLAN は、制限 VLAN として設定することができません。1 つの VLAN を制限 VLAN と音声 VLAN の両方として指定することはできません。

制限 VLAN での再認証をイネーブルにします。再認証がディセーブルになっていると、制限 VLAN 内のポートは認証要求を受信しません。

再認証プロセスを開始するには、制限 VLAN がポートからリンクダウン イベントまたは Extensible Authentication Protocol (EAP) ログオフ イベントを受け取る必要があります。ホストがハブを介して接続されている場合は、次の動作が発生する可能性があります。

- ホストが切断されているとポートがリンクダウン イベントを受け取らない
- 次の再認証が実行されるまでポートが新しいホストを検出しない

制限 VLAN をタイプの異なる VLAN として再設定すると、制限 VLAN のポートは現在許可されたステータスのまま移行します。

例

次の例では、**authentication event fail** コマンドを設定する方法を示します。

```
Switch(config)# authentication event fail action authorize vlan 20
```

次の例では、no-response アクションを設定する方法を示します。

```
Switch(config)# authentication event no-response action authorize vlan 10
```

次の例では、server-response アクションを設定する方法を示します。

```
Switch(config)# authentication event server alive action reinitialize
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単方向モードまたは双方向モードに設定します。
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン 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	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上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	ポートの許可ステータスの手動制御をイネーブルにします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication fallback

クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定するには、**authentication fallback** 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。

authentication fallback *name*

no authentication fallback *name*

シンタックスの説明

<i>name</i>	Web 認証のフォールバック プロファイルを指定します。
-------------	------------------------------

デフォルト

フォールバックはイネーブルではありません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

フォールバック方式を設定する前に、**authentication port-control auto** 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必要があります。

Web 認証は、802.1x または MAB フォールバック方式としてのみ設定できます。したがって、これらの認証方式の一方または両方を、イネーブルにするフォールバック方式として設定する必要があります。

例

次の例では、ポート上でフォールバック プロファイルを指定する方法を示します。

```
Switch(config)# authentication fallback profile1
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン 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	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上で再認証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 port-control	ポートの許可ステータスの手動制御をイネーブルにします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication host-mode

ポート上で認証マネージャ モードを設定するには、**authentication host-mode** 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。

authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]

no authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]

シンタックスの説明

multi-auth	ポート上で複数認証モード (multiauth モード) をイネーブルにします。
multi-domain	ポート上で複数ドメイン モードをイネーブルにします。
multi-host	ポート上で複数ホスト モードをイネーブルにします。
single-host	ポート上で単一ホスト モードをイネーブルにします。

デフォルト

単一ホスト モードがイネーブルになっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

1 つのデータ ホストしか接続されていない場合は、単一ホスト モードに設定する必要があります。単一ホスト ポート上での認証用に音声デバイスを接続しないでください。ポート上に音声 VLAN が設定されていないと、音声デバイスの許可が正常に実行されません。

データ ホストが IP Phone を経由してポートに接続されている場合は、複数ドメイン モードに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、複数ドメイン モードに設定する必要があります。

ハブの背後に最大 8 台のデバイスを配置し、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、複数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 台だけです。

複数ホスト モードでは、ハブの背後にある複数のホストへのポート アクセスに対応していますが、最初のユーザの認証後にこれらのデバイスへのポート アクセスが無制限になります。

例

次の例では、ポート上で **multiauth** モードをイネーブルにする方法を示します。

```
Switch(config)# authentication host-mode multi-auth
```

次の例では、ポート上で **multi-domain** モードをイネーブルにする方法を示します。

```
Switch(config)# authentication host-mode multi-domain
```

次の例では、ポート上で **multi-host** モードをイネーブルにする方法を示します。

Switch(config)# **authentication host-mode multi-host**

次の例では、ポート上で **single-host** モードをイネーブルにする方法を示します。

Switch(config)# **authentication host-mode single-host**

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication open	ポート上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	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上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	ポートの許可ステータスの手動制御をイネーブルにします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication open

ポート上でオープン アクセスをイネーブルまたはディセーブルにするには、**authentication open** 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。オープン アクセス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。

authentication open

no authentication open

デフォルト

オープン アクセスがディセーブルになっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

認証の前にデバイスでネットワーク アクセスが必要となる場合は、オープン認証をイネーブルにする必要があります。

ポート ACL を使用して、オープン認証がイネーブルになっている場合にホスト アクセスを制限する必要があります。

例

次の例では、ポート上でオープン アクセスをイネーブルにする方法を示します。

```
Switch(config)# authentication open
```

次の例では、ポート上でオープン アクセスがディセーブルになるようにポートを設定する方法を示します。

```
Switch(config)# no authentication open
```

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication order	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上で再認証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 port-control	ポートの許可ステータスの手動制御をイネーブルにします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication order

ポート上で使用される認証方式の順序を設定するには、**authentication order** 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。

authentication order [dot1x | mab] {webauth}

no authentication order

シンタックスの説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	認証方式の順序に MAC Authentication Bypass (MAB; MAC 認証バイパス) を追加します。
webauth	認証方式の順序に Web 認証を追加します。

コマンドのデフォルト

デフォルトの認証順序では、**dot1x** のあとに **mab** と **webauth** が配置されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

順序付けでは、ポートに接続される新しいデバイスを認証する場合にスイッチが試行する認証方式の順序を設定します。リスト内の 1 つの認証方式の試行に失敗すると、次の方式が試行されます。

それぞれの認証方式は一度しか入力できません。802.1x と MAB の間でのみ柔軟な順序付けが可能です。

Web 認証は、独立した方式として設定することも、順序内で 802.1x または MAB のあとに配置される最後の方式として設定することもできます。Web 認証は、**dot1x** または **mab** のフォールバックとしてのみ設定する必要があります。

例

次の例では、802.1x を最初の認証方式として追加し、MAB を 2 番目の認証方式として追加し、Web 認証を 3 番目の認証方式として追加する方法を示します。

```
Switch(config)# authentication order dotx mab webauth
```

次の例では、MAC 認証バイパス (MAB) を最初の認証方式として追加し、Web 認証を 2 番目の認証方式として追加する方法を示します。

```
Switch(config)# authentication order mab webauth
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン アクセスをイネーブルまたはディセーブルにします。
authentication periodic	ポート上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	ポートの許可ステータスの手動制御をイネーブルにします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
mab	ポート上で MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol (EAP) を使用するようにポートを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication periodic

ポート上で再認証をイネーブルまたはディセーブルにするには、**authentication periodic** 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。再認証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。

authentication periodic

no authentication periodic

コマンドのデフォルト 再認証がディセーブルになっています。

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン **authentication timer 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、定期的な再認証の試行間隔を設定します。

例 次の例では、ポート上で定期的な再認証をイネーブルにする方法を示します。

```
Switch(config)# authentication periodic
```

次の例では、ポート上で定期的な再認証をディセーブルにする方法を示します。

```
Switch(config)# no authentication periodic
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
	authentication event	特定の認証イベントに対するアクションを設定します。
	authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
	authentication host-mode	ポート上で認証マネージャ モードを設定します。
	authentication open	ポート上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	ポート上で使用される認証方式の順序を設定します。
	authentication port-control	ポートの許可ステータスの手動制御をイネーブルにします。
	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。

コマンド	説明
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication port-control

ポートの許可ステータスの手動制御をイネーブルにするには、**authentication 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 port-control {auto | force-authorized | force-un authorized}

no authentication port-control {auto | force-authorized | force-un authorized}

シンタックスの説明

auto	ポート上で IEEE 802.1x 認証をイネーブルにします。スイッチとクライアント間の IEEE 802.1x 認証交換に基づいてポートが許可ステータスまたは無許可ステータスに切り替えられます。
force-authorized	ポート上で IEEE 802.1x 認証をディセーブルにします。認証交換なしでポートが許可ステータスに切り替えられます。ポートはクライアントとの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
force-un authorized	ポートへのアクセスをすべて拒否します。ポートが無許可ステータスに切り替えられ、クライアントの認証試行がすべて無視されます。スイッチはポートを介してクライアントに認証サービスを提供できません。

デフォルト

デフォルトの設定は **force-authorized** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

これらのポート タイプのいずれかでのみ **auto** キーワードを使用します。

- **トランク ポート**：トランク ポート上で 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 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、エラーメッセージが表示され、ポート モードは変更されません。
- **ダイナミック ポート**：ダイナミック ポートは、ネイバーとネゴシエートしてトランク ポートになる場合があります。ダイナミック ポート上で 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。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラーメッセージが表示され、ポート モードは変更されません。
- **ダイナミック アクセス ポート**：ダイナミック アクセス (VLAN Query Protocol [VQP]) 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。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。

- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバーを 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と、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。
- Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN; リモート SPAN) 宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままになります。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。

スイッチの IEEE 802.1x 認証をグローバルにディセーブルにするには、**no dot1x system-auth-control** 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。特定のポート上で IEEE 802.1x 認証をディセーブルにするか、またはデフォルト設定に戻すには、**no authentication port-control** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポート ステートを **auto** に設定する方法を示します。

```
Switch(config)# authentication port-control auto
```

次の例では、ポート ステートを **force-authorized** に設定する方法を示します。

```
Switch(config)# authentication port-control force-authorized
```

次の例では、ポート ステートを **force-unauthorized** に設定する方法を示します。

```
Switch(config)# authentication port-control force-unauthorized
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン 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	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上で再認証をイネーブルまたはディセーブルにします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication priority

認証方式をポート プライオリティ リストに追加するには、**authentication priority** 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。

```
auth priority [dot1x | mab] {webauth}
```

```
no auth priority [dot1x | mab] {webauth}
```

シンタックスの説明

dot1x	認証方式の順序に 802.1x を追加します。
mab	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。

コマンドのデフォルト

デフォルトのプライオリティは 802.1x 認証です。MAC 認証バイパスと Web 認証がそのあとに続きます。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

順序付けでは、ポートに接続される新しいデバイスを認証する場合にスイッチが試行する認証方式の順序を設定します。

ポート上で複数のフォールバック方式を設定する場合は、Web 認証 (webauth) を最後に設定します。それぞれの認証方式にプライオリティを割り当てると、プライオリティの低い認証方式の実行中にプライオリティの高い認証方式を割り込ませることができます。



(注)

クライアントが認証済の場合にプライオリティの高い認証方式による割り込みが発生すると、そのクライアントの再認証が実行されることがあります。

認証方式のデフォルト プライオリティは、実行リストの順序内の配置と同じになります (つまり、802.1x 認証、MAC 認証バイパス、Web 認証の順になります)。デフォルトの順序を変更するには、**dot1x**、**mab**、および **webauth** キーワードを使用します。

例

次の例では、802.1x を最初の認証方式として設定し、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。

```
Switch(config)# authentication priority dotx webauth
```

次の例では、MAC 認証バイパス (MAB) を最初の認証方式として設定し、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。

```
Switch(config)# authentication priority mab webauth
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン 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	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上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	ポートの許可ステータスの手動制御をイネーブルにします。
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された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
mab	ポート上で MAC 認証バイパスをイネーブルにします。
mab eap	Extensible Authentication Protocol (EAP) を使用するようにポートを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

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するには、**authentication timer** 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。

```
authentication timer {[inactivity | reauthenticate] [server | am]} {restart value}
no authentication timer {[inactivity | reauthenticate] [server | am]} {restart value}
```

シンタックスの説明

inactivity	アクティビティが存在しない場合にクライアントが無許可になるまでの間隔 (秒) を指定します。
reauthenticate	再認証が自動的に試行されるまでの間隔 (秒) を指定します。
server	無許可ポートの認証が試行されるまでの間隔 (秒) を指定します。
restart	無許可ポートの認証が試行されるまでの間隔 (秒) を指定します。
value	1 ~ 65535 (秒) の値を入力します。

デフォルト

inactivity、**server**、および **restart** キーワードがオフに設定されています。**reauthenticate** キーワードが 1 時間に設定されています。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

タイムアウト値を設定しないと、802.1x セッションが無期限に許可された状態になります。この場合は、他のホストがそのポートを使用することも、接続されているホストが同じスイッチ上の別のポートに移動することもできません。

例

次の例では、認証非アクティブ タイマーを 60 秒に設定する方法を示します。

```
Switch(config)# authentication timer inactivity 60
```

次の例では、再認証タイマーを 120 秒に設定する方法を示します。

```
Switch(config)# authentication timer restart 120
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。

コマンド	説明
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン アクセスをイネーブまたはディセーブにします。
authentication order	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上で再認証をイネーブまたはディセーブにします。
authentication port-control	ポートの許可ステートの手動制御をイネーブにします。
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 violation	新しいデバイスがポートに接続された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定します。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

authentication violation

新しいデバイスがポートに接続された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定するには、**authentication violation** 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。

authentication violation {protect | restrict | shutdown}

no authentication violation {protect | restrict | shutdown}

シンタックスの説明

protect	予期しない着信 MAC アドレスが廃棄されます。Syslog エラーは生成されません。
restrict	違反エラーが発生したときに Syslog エラーを生成します。
shutdown	予期しない MAC アドレスが生成されたポートまたは仮想ポートを errdisable にします。

デフォルト

デフォルトでは、**authentication violation shutdown** モードがイネーブルになっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、IEEE 802.1x 対応ポートを errdisable として設定し、新しいデバイスがそのポートに接続された時点でシャットダウンする方法を示します。

```
Switch(config-if)# authentication violation shutdown
```

次の例では、新しいデバイスがポートに接続された場合にシステム エラー メッセージを生成し、制限モードに切り替わるように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation restrict
```

次の例では、新しいデバイスがポートに接続された場合にそのデバイスを無視するように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation protect
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。

コマンド	説明
authentication fallback	クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン アクセスをイネーブまたはディセーブにします。
authentication order	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上で再認証をイネーブまたはディセーブにします。
authentication port-control	ポートの許可ステートの手動制御をイネーブにします。
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。
show authentication	スイッチ上の認証マネージャ イベントに関する情報を表示します。

auto qos voip

QoS (Quality Of Service) ドメイン内の Voice over IP (VoIP) に対して QoS を自動的に設定するには、**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。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]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

cisco-phone	このポートが Cisco IP Phone に接続されていると判断し、自動的に VoIP の QoS 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	このポートが Cisco SoftPhone を実行しているデバイスに接続されていると判断し、自動的に VoIP の QoS を設定します。
trust	このポートが信頼できるスイッチまたはルータに接続されていると識別し、自動的に VoIP の QoS 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。

デフォルト

Auto-QoS は、ポート上でディセーブルに設定されています。

auto-QoS がイネーブルの場合は、表 2-1 に示すように、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。

表 2-1 トラフィック タイプ、パケット ラベル、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 ¹ BPDU ² 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 ³	46	24、26	48	56	34	—	
CoS ⁴	5	3	6	7	3	—	
CoS から入力 キューへのマッ ピング	2、3、4、5、6、7 (キュー 2)					0、1 (キュー 1)	
CoS から出力 キューへのマッ ピング	5 (キュー 1)	3、6、7 (キュー 2)			4 (キュー 3)	2 (キュー 3)	0、1 (キュー 4)

1. STP = スパニング ツリー プロトコル
2. BPDU = ブリッジ プロトコル データ ユニット
3. DSCP = Diffserve コード ポイント
4. CoS = サービス クラス

表 2-2 に、入力キューに対して生成された Auto-QoS の設定を示します。

表 2-2 入力キューに対する Auto-QoS の設定

入力キュー	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)	キュー (バッファ) サイズ
SRR ¹ 共有	1	0、1	81%	67%
プライオリティ	2	2、3、4、5、6、7	19%	33%

1. SRR = シェイプド ラウンド ロビン。入力キューは共有モードのみサポートします。

表 2-3 に、出力キューに対して生成される auto-QoS の設定を示します。

表 2-3 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 (シェーピング)	1	5	最大 100%	16%	10%
SRR 共有	2	3、6、7	10%	6%	10%
SRR 共有	3	2、4	60%	17%	26%
SRR 共有	4	0、1	20%	61%	54%

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	コマンド出力の情報が変更されました。
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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、スイッチ、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装置などが含まれます。

auto-QoS は、スイッチおよびルーテッドポート上の Cisco IP Phone を使用した VoIP と、Cisco SoftPhone アプリケーションが動作する装置を使用した VoIP に対してスイッチを設定します。これらのリリースでは、Cisco IP SoftPhone バージョン 1.3(3) 以降のみがサポートされます。接続されたデバイスは、Cisco Call Manager バージョン 4 以降を使用している必要があります。

show auto qos コマンド出力では、Cisco IP Phone のサービス ポリシー情報が表示されます。

Auto-QoS のデフォルトを利用する場合、他の QoS コマンドを設定する前に、Auto-QoS をイネーブルにする必要があります。Auto-QoS をイネーブルにしたあとに、Auto-QoS 設定の調整をすることができます。



(注)

スイッチは Auto-QoS で生成されたコマンドを、Command-Line Interface (CLI; コマンドライン インターフェイス) からの入力のように適用します。既存のユーザ設定では、生成されたコマンドの適用が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。(これらは警告なしで行われます)。生成されたコマンドが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が、実行中の設定に残っています。上書きしてしまったユーザ入力の設定は、現行の設定をメモリに保存せずにスイッチをリロードすることによって、復旧することができます。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。他のポート上で Auto-QoS をイネーブルにした場合、Auto-QoS が生成するインターフェイス コンフィギュレーション コマンドは、そのポート用に実行されます。

最初のポート上で Auto-QoS 機能をイネーブルにした場合、次のアクションが自動的に起こります。

- QoS がグローバルにイネーブルになり (**mls qos** グローバル コンフィギュレーション コマンド)、そのあと、他のグローバル コンフィギュレーション コマンドが追加されます。

スイッチ ポートが Cisco IOS Release 12.2(37)SE かそれよりも前のリリースで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを使用して設定された場合、auto-QoS によって Cisco IOS Release 12.2(40)SE に新しく生成されたコマンドは、ポートに適用されません。このようなコマンドを自動的に適用するには、設定を削除してからポートに再度適用する必要があります。

- Cisco SoftPhone を実行しているデバイスに接続されたネットワークのエッジにあるポート上で、**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、スイッチはポリシングを使用してパケットがイン プロファイルであるかアウト オブ プロファイルであるかを判別し、パケット上でのアクションを指定します。パケットに 24、26、または 46 の DSCP 値がない場合またはパケットがアウト オブ プロファイルの場合は、スイッチで DSCP 値が 0 に変更されます。スイッチは、表 2-2 および表 2-3 の設定値に従ってポートの入力キューと出力キューを設定します。
- 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、スイッチは入力パケットでルーティングされないポートの CoS 値を信頼します (トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります)。スイッチは、表 2-2 および表 2-3 の設定値に従ってポートの入力キューと出力キューを設定します。

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 ポートにある Cisco IP Phone で auto-QoS をイネーブルにする場合、スタティック IP アドレスを IP Phone に割り当てる必要があります。



(注)

Cisco SoftPhone を実行しているデバイスがスイッチ ポートまたはルーテッド ポートに接続されている場合、スイッチがサポートするのはポートあたり 1 つの Cisco SoftPhone アプリケーションのみです。

Auto-QoS をイネーブルにしたあと、名前に *AutoQoS* を含むポリシーマップまたは集約ポリサーを変更しないでください。ポリシーマップまたは集約ポリサーを変更する必要がある場合は、ポリシーマップまたは集約ポリサーをコピーし、そのコピーを変更します。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、生成されたポリシーマップをインターフェイスから削除し、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。Auto-QoS のデバッグをイネーブルにするには、**debug auto qos** 特権 EXEC コマンドを使用します。詳細については、**debug auto qos** コマンドを参照してください。

ポート上で 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。このポート用に生成された Auto-QoS インターフェイス コンフィギュレーション コマンドのみ削除されます。Auto-QoS がイネーブルである最後のポートで **no auto qos voip** コマンドを入力した場合、Auto-QoS 生成のグローバル コンフィギュレーション コマンドが残っていたとしても、Auto-QoS はディセーブルになったと認識されます（グローバル コンフィギュレーションに影響を受ける他のポートのトラフィック障害を回避するため）。**no mls qos** 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、Auto-QoS 生成のグローバル コンフィギュレーション コマンドをディセーブルにします。QoS がディセーブルの場合、パケットが修正されなくなるため（パケットの CoS、DSCP、IP precedence の値は変更されない）、ポートの信頼性に関する概念はなくなります。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベストエフォートに分類されます）。

例

次の例では、ポートに接続されているスイッチまたはルータが信頼できる装置である場合に、auto-QoS をイネーブルにし、着信パケットで受信した QoS ラベルを信頼する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip trust
```

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。

関連コマンド

コマンド	説明
debug auto qos	Auto-QoS 機能のデバッグをイネーブルにします。
mls qos cos	デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。
mls qos map {cos-dscp dscp1 ... dscp8 dscp-cos dscp-list to cos}	CoS から DSCP へのマッピングまたは DSCP から CoS へのマッピングを定義します。
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	DSCP 値を出力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos trust	ポートの信頼状態を設定します。
queue-set	キューセットに対しポートをマッピングします。
show auto qos	auto-QoS 情報を表示します。

コマンド	説明
<code>show mls qos interface</code>	ポート レベルで QoS 情報を表示します。
<code>srr-queue bandwidth shape</code>	シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅のシェーピングをイネーブルにします。
<code>srr-queue bandwidth share</code>	共有ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

boot 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指定するには、**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。

boot config-file flash:/file-url

no boot config-file

シンタックスの説明

flash:/file-url コンフィギュレーション ファイルのパス (ディレクトリ) および名前

デフォルト

デフォルトのコンフィギュレーション ファイルは、flash:config.text です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

このコマンドは、CONFIG_FILE 環境変数の設定を変更します。詳細については、[付録 A 「Catalyst 2960 スイッチ ブートローダ コマンド」](#) を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot enable-break

自動ブートプロセスの中断をイネーブルにするには、**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。

boot enable-break

no boot enable-break

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル。コンソール上で **Break** キーを押しても自動ブートプロセスを中断することはできません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力すると、フラッシュ ファイル システムが初期化されたあとで **Break** キーを押すことにより、自動ブートプロセスを中断することができます。



(注)

このコマンドの設定に関係なく、スイッチ前面パネルの **MODE** ボタンを押せば、いつでも自動ブートプロセスを中断することができます。

このコマンドは、**ENABLE_BREAK** 環境変数の設定を変更します。詳細については、[付録 A 「Catalyst 2960 スイッチ ブートローダ コマンド」](#) を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper

ブートローダの初期化中に動的にファイルをロードして、ブートローダの機能を拡張するか、またはブートローダの機能にパッチを当てるには、**boot helper** グローバル コンフィギュレーション コマンドを使用します。このコマンドをデフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

boot helper *filesystem:/file-url ...*

no boot helper

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: を使用します。
<i>/file-url</i>	ローダ初期化中に動的にロードするためのパス (ディレクトリ) およびロード可能なファイルのリスト。イメージ名はセミコロンで区切ります。

デフォルト

ヘルパー ファイルはロードされません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

この変数は、内部開発およびテスト専用です。

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

このコマンドは、HELPER 環境変数の設定を変更します。詳細については、[付録 A 「Catalyst 2960 スイッチ ブートローダ コマンド」](#) を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot helper-config-file

Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前を指定するには、**boot helper-config-file** グローバル コンフィギュレーション コマンドを使用します。このコマンドが設定されていない場合は、CONFIG_FILE 環境変数によって指定されたファイルがロードされたすべてのバージョンの Cisco IOS に使用されます。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。

boot helper-config-file *filesystem:/file-url*

no boot helper-config file

シンタックスの説明	説明
<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボードフラッシュ デバイスに対して flash: を使用します。
<i>/file-url</i>	ロードするパス (ディレクトリ) およびヘルパー コンフィギュレーション ファイル

デフォルト ヘルパー コンフィギュレーション ファイルは指定されません。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン この変数は、内部開発およびテスト専用です。
ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
このコマンドは、HELPER_CONFIG_FILE 環境変数の設定を変更します。詳細については、[付録 A 「Catalyst 2960 スイッチ ブートローダ コマンド」](#) を参照してください。

関連コマンド	コマンド	説明
	show boot	BOOT 環境変数の設定を表示します。

boot manual

次回ブート サイクル中にスイッチの手動起動をイネーブルにするには、**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。

boot manual

no boot manual

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

手動による起動はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

次回システムを再起動すると、スイッチはブートローダ モードで起動します。このことは *switch:* プロンプトで確認できます。システムを起動するには、**boot** ブート ローダ コマンドを使用して起動可能なイメージの名前を指定します。

このコマンドは、MANUAL_BOOT 環境変数の設定を変更します。詳細については、[付録 A 「Catalyst 2960 スイッチ ブートローダ コマンド」](#) を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

boot private-config-file

Cisco IOS がプライベート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するには、**boot private-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。

boot private-config-file *filename*

no boot private-config-file

シンタックスの説明	<i>filename</i>	プライベート コンフィギュレーション ファイルの名前
-----------	-----------------	----------------------------

デフォルト	デフォルトのコンフィギュレーション ファイルは、 <i>private-config</i> です。
-------	--

コマンド モード	グローバル コンフィギュレーション
----------	-------------------

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン	ファイル名では、大文字と小文字が区別されます。
------------	-------------------------

例	次の例では、プライベート コンフィギュレーション ファイルの名前を <i>pconfig</i> と指定する方法を示します。
---	--

```
Switch(config)# boot private-config-file pconfig
```

関連コマンド	コマンド	説明
	show boot	BOOT 環境変数の設定を表示します。

boot system

次のブート サイクル中にロードする Cisco IOS イメージを指定するには、**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。

```
boot system filesystem:/file-url ...
```

```
no boot system
```

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: 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。

デフォルト

スイッチは、BOOT 環境変数内の情報を使用して、自動的にシステムの起動を試みます。この変数が設定されていない場合、スイッチは、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、最初の実行可能イメージをロードして実行しようとしています。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。

archive download-sw 特権 EXEC コマンドを使用してシステム イメージを保存している場合、**boot system** コマンドを使用する必要はありません。**boot system** コマンドは自動的に処理され、ダウンロードされたイメージがロードされます。

このコマンドは、BOOT 環境変数の設定を変更します。詳細については、[付録 A 「Catalyst 2960 スイッチ ブートロード コマンド」](#) を参照してください。

関連コマンド

コマンド	説明
show boot	BOOT 環境変数の設定を表示します。

channel-group

EtherChannel グループにイーサネット ポートを割り当てたり、EtherChannel モードをイネーブルにしたりするには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用します。イーサネット ポートを EtherChannel グループから削除する場合は、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

PAGP modes:

channel-group *channel-group-number* **mode** {{**auto** [**non-silent**]} | {**desirable** [**non-silent**]}}

LACP modes:

channel-group *channel-group-number* **mode** {**active** | **passive**}

On mode:

channel-group *channel-group-number* **mode on**

シンタックスの説明

channel-group-number	チャネルグループ番号を指定します。指定できる範囲は 1 ～ 6 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。 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。この場合、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	Port Aggregation Protocol (PAgP; ポート集約プロトコル) 装置が検出された場合にかぎり、PAgP をイネーブルにします。 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	PAgP を無条件でイネーブルにします。 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、デフォルトでサイレント動作となります。
non-silent	(任意) 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。

channel-group

on	<p>on モードをイネーブルにします。</p> <p>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。</p>
passive	<p>LACP 装置が検出された場合にかぎり、LACP をイネーブルにします。</p> <p>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。</p>

デフォルト

チャンネルグループは割り当てられません。
モードは設定されていません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 EtherChannel の場合、物理ポートをチャンネルグループに割り当てる前に、先に **interface port-channel** 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ートチャンネル インターフェイスを作成しておく必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。論理インターフェイスがまだ作成されていない場合は、チャンネルグループが最初の物理ポートを取得した時点で、自動的にポートチャンネル インターフェイスが作成されます。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** と同じ番号を使用することもできれば、新しい番号を使用することもできます。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。

EtherChannel を設定したあと、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のみに有効です。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 をリンクとして設定します。

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することができます。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、**on** モードのポートグループが、**on** モードの別のポートグループに接続する場合だけです。



注意

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ンニングツリーのループが発生することがあります。

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 を稼動している EtherChannel グループと LACP を稼動している EtherChannel グループが同一スイッチ上に共存してもかまいません。個々の EtherChannel グループは PAgP または LACP のどちら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。

アクティブまたはアクティブでない EtherChannel メンバーを 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と、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」を参照してください。

例

次の例では、EtherChannel を設定する方法を示します。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。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

次の例では、EtherChannel を設定する方法を示します。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。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

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。

関連コマンド

コマンド	説明
channel-protocol	チャネリングを管理するため、ポート上で使用されるプロトコルを制限します。
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。
show etherchannel	チャンネルの EtherChannel 情報を表示します。
show lacp	LACP チャネル グループ情報を表示します。

コマンド	説明
show pagp	PAgP チャンネル グループ情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」> 「File Management Commands」> 「Configuration File Management Commands」を選択してください。

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、**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

シンタックスの説明

lacp	Link Aggregation Control Protocol (LACP) で EtherChannel を設定します。
pagp	ポート集約プロトコル (PAgP) で EtherChannel を設定します。

デフォルト

EtherChannel に割り当てられているプロトコルはありません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

channel-protocol コマンドは、チャネルを LACP または PAgP に制限するためのみに使用します。**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 **channel-group** インターフェイス コンフィギュレーション コマンドで上書きされることはありません。

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。

例

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。

```
Switch(config-if)# channel-protocol lacp
```

show etherchannel [channel-group-number] protocol 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel protocol	EtherChannel のプロトコル情報を表示します。

cisp enable

スイッチ上で Client Information Signalling Protocol (CISP) をイネーブルにして、サブリカントスイッチのオーセンティケータ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

シンタックスの説明

cisp enable	CISP をイネーブルにします。
--------------------	------------------

デフォルト

デフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

オーセンティケータとサブリカントスイッチ間のリンクはトランクになります。両方のスイッチ上で VTP をイネーブルにする場合は、VTP ドメイン名を同じにして、VTP モードを *server* にする必要があります。

VTP モードを設定したら、MD5 チェックサム不一致エラーが発生しないようにするために次のことを確認してください。

- 2 つの異なるスイッチ上に VLAN がそれぞれ設定されていない (2 つの VTP サーバが同じドメイン内に存在することが原因と考えられる)
- 2 つのスイッチに異なるコンフィギュレーション リビジョン番号が設定されている

例

次の例では、CISP をイネーブルにする方法を示します。

```
switch(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentials (グローバルコンフィギュレーション) profile	サブリカントスイッチのプロファイルを設定します。
show cisp	特定のインターフェイスの CISP 情報を表示します。

class

指定されたクラス マップ名のトラフィック分類一致条件 (**police**、**set**、および **trust** ポリシー マップ クラス コンフィギュレーション コマンドによる) を定義するには、**class** 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*

no class *class-map-name*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>class-map-name</i>	クラス マップ名です。
-----------------------	-------------

デフォルト

ポリシーマップ クラス マップは定義されません。

コマンド モード

ポリシーマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 マップをポートへ適用できます。

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。

- **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。詳細については、[police](#) および [police aggregate](#) ポリシー マップ クラス コマンドを参照してください。
- **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。
- **trust** : **class** コマンドまたは **class-map** コマンドで分類したトラフィックの信頼状態を定義します。詳細については、[trust](#) コマンド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。

例

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。このコマンドが入力方向に添付された場合、*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、IP Differentiated Services Code Point (DSCP; DiffServ コード ポイント) を 10 に設定し、平均レート 1 Mbps、バースト 20 KB のトラフィックをポリシングします。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# 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。

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの比較に使用されるクラス マップを作成します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー マップを作成または変更します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	QoS (Quality Of Service) ポリシー マップを表示します。
trust	class ポリシーマップ コンフィギュレーション コマンドまたは class-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分類されたトラフィックの信頼状態を定義します。

class-map

パケットと指定したクラス名と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、**class-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 モードに戻る場合は、このコマンドの **no** 形式を使用します。

class-map [**match-all** | **match-any**] *class-map-name*

no class-map [**match-all** | **match-any**] *class-map-name*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

match-all	(任意) このクラス マップ内のすべての一致ステートメントの論理積をとります。クラス マップ内のすべての基準が一致する必要があります。
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 つまたは複数の条件が一致していなければなりません。
<i>class-map-name</i>	クラス マップ名です。

デフォルト

クラス マップは定義されません。

match-all または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

クラス マップ一致基準を作成または変更したい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。

QoS (Quality Of Service) クラスマップ コンフィギュレーション モードでは、次の設定コマンドを利用できます。

- **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。詳細については、**match** (クラス マップ コンフィギュレーション) コマンドを参照してください。

- **no** : クラス マップから **match** 文を削除します。
- **rename** : 現在のクラス マップの名前を変更します。クラス マップ名をすでに使用されている名前に変更すると、A class-map with this name already exists が表示されます。

物理ポート単位でパケット分類を定義するため、クラス マップごとに 1 つずつのみ **match** コマンドがサポートされています。この状況では、**match-all** キーワードと **match-any** キーワードは同じです。

1 つのクラス マップで設定できるアクセス コントロール リスト (ACL) は 1 つだけです。ACL には複数の Access Control Entry (ACE; アクセス コントロール エントリ) を含めることができます。

例

次の例では、クラス マップ *class1* に 1 つの一致基準 (アクセス リスト 103) を設定する方法を示します。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

次の例では、クラス マップ *class1* を削除する方法を示します。

```
Switch(config)# no class-map class1
```

show class-map 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件 (police 、 set 、および trust ポリシーマップ クラス コンフィギュレーション コマンドによる) を定義します。
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条件を定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー マップを作成または変更します。
show class-map	QoS クラス マップを表示します。

clear dot1x

スイッチまたは指定されたポートの IEEE 802.1x 情報をクリアするには、**clear dot1x** 特権 EXEC コマンドを使用します。

```
clear dot1x {all | interface interface-id}
```

シンタックスの説明

all	スイッチのすべての IEEE 802.1x 情報をクリアします。
interface interface-id	指定されたインターフェイスの IEEE 802.1x 情報をクリアします。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

clear dot1x all コマンドを使用して、すべての情報をクリアできます。また、**clear dot1x interface interface-id** コマンドを使用して、指定されたインターフェイスの情報のみをクリアできます。

例

次の例では、すべての IEEE 802.1x 情報をクリアする方法を示します。

```
Switch# clear dot1x all
```

次の例では、指定されたインターフェイスの IEEE 802.1x 情報をクリアする方法を示します。

```
Switch# clear dot1x interface gigabithethernet0/1
```

情報が削除されたかどうかを確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x	スイッチ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します。

clear eap sessions

スイッチまたは指定されたポートの Extensible Authentication Protocol (EAP) セッション情報をクリアするには、**clear eap sessions** 特権 EXEC コマンドを使用します。

```
clear eap sessions [credentials name [interface interface-id] | interface interface-id |
method name | transport name] [credentials name | interface interface-id | transport name] ...
```

シンタックスの説明

credentials name	指定されたプロファイルの EAP クレデンシャル情報をクリアします。
interface interface-id	指定されたインターフェイスの EAP 情報をクリアします。
method name	指定された方式の EAP 情報をクリアします。
transport name	指定された下位レベルの EAP トランスポート情報をクリアします。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

clear eap sessions コマンドを使用して、すべてのカウンタをクリアできます。キーワードを指定して、特定の情報のみをクリアできます。

例

次の例では、すべての EAP 情報をクリアする方法を示します。

```
Switch# clear eap
```

次の例では、指定されたプロファイルの EAP セッション クレデンシャル情報をクリアする方法を示します。

```
Switch# clear eap sessions credential type1
```

情報が削除されたかどうかを確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show eap	スイッチまたは特定のポートの EAP のレジストレーション情報およびセッション情報を表示します。

clear energywise neighbors

EnergyWise ネイバー テーブルを削除するには、**clear energywise neighbors** 特権 EXEC コマンドを使用します。

clear energywise neighbors

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

例 次の例では、ネイバー テーブルを削除する方法を示します。

```
Switch# clear energywise neighbors  
Cleared all non static energywise neighbors
```

テーブルが削除されたかどうかを確認するには、**show energywise neighbors** 特権 EXEC コマンドを使用します。

関連コマンド	コマンド	説明
	show energywise neighbors	EnergyWise ネイバー テーブルを表示します。

clear errdisable interface

errdisable になった VLAN をもう一度イネーブルにするには、**clear errdisable interface** 特権 EXEC コマンドを使用します。

clear errdisable interface *interface-id* **vlan** [*vlan-list*]

シンタックスの説明

<i>vlan list</i>	(任意) 再びイネーブルにする VLAN のリストを指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。
------------------	--

コマンドのデフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

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 interface** コマンドを使用して VLAN の errdisable をクリアできます。

例

次の例では、errdisable ステートになっているポート Gi0/2 上のすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface GigabitEthernet0/2 vlan
```

関連コマンド

コマンド	説明
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リストのインターフェイス ステータスを表示します。

clear arp inspection log

clear ip arp inspection log 特権 EXEC コマンドを使用して、ダイナミック アドレス解決プロトコル (ARP) インスペクションのログ バッファをクリアします。

clear ip arp inspection log

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

例 次の例では、ログ バッファの内容をクリアする方法を示します。

```
Switch# clear ip arp inspection log
```

ログがクリアされたかどうかを確認するには、**show ip arp inspection log** 特権コマンドを入力します。

関連コマンド	コマンド	説明
	arp access-list	ARP アクセス コントロール リスト (ACL) を定義します。
	ip arp inspection log-buffer	ダイナミック ARP インスペクションのログ バッファを設定します。
	ip arp inspection vlan logging	VLAN ごとにロギングされるパケットのタイプを制御します。
	show inventory log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

clear ip arp inspection statistics

ダイナミック アドレス解決プロトコル (ARP) インスペクション統計情報をクリアするには、**clear ip arp inspection statistics** 特権 EXEC コマンドを使用します。

clear ip arp inspection statistics [vlan vlan-range]

シンタックスの説明	vlan vlan-range (任意) 指定された VLAN (1 つまたは複数) の統計情報をクリアします。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
------------------	---

デフォルト デフォルトは定義されていません。

コマンドモード 特権 EXEC

コマンドの履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>12.2(50)SE</td> <td>このコマンドが追加されました。</td> </tr> </tbody> </table>	リリース	変更内容	12.2(50)SE	このコマンドが追加されました。
リリース	変更内容				
12.2(50)SE	このコマンドが追加されました。				

例 次の例では、VLAN 1 の統計情報をクリアする方法を示します。

```
Switch# clear ip arp inspection statistics vlan 1
```

統計情報が削除されたかどうかを確認するには、**show ip arp inspection statistics vlan 1** 特権 EXEC コマンドを入力します。

関連コマンド	<table border="1"> <thead> <tr> <th>コマンド</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>show inventory statistics</td> <td>すべての VLAN または指定された VLAN に関して転送されたパケット、廃棄されたパケット、MAC 検証で不合格となったパケット、および IP 検証で不合格となったパケットの統計情報を表示します。</td> </tr> </tbody> </table>	コマンド	説明	show inventory statistics	すべての VLAN または指定された VLAN に関して転送されたパケット、廃棄されたパケット、MAC 検証で不合格となったパケット、および IP 検証で不合格となったパケットの統計情報を表示します。
コマンド	説明				
show inventory statistics	すべての VLAN または指定された VLAN に関して転送されたパケット、廃棄されたパケット、MAC 検証で不合格となったパケット、および IP 検証で不合格となったパケットの統計情報を表示します。				

clear ip dhcp snooping

DHCP スヌーピング バインディング データベース、DHCP スヌーピング バインディング データベース エージェントの統計情報、または DHCP スヌーピング 統計カウンタをクリアするには、**clear ip dhcp snooping** 特権 EXEC コマンドを使用します。

clear ip dhcp snooping {**binding** {* | *ip-address* | **interface** *interface-id* | **vlan** *vlan-id*} | **database statistics** | **statistics**}



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

binding	DHCP スヌーピング バインディング データベースをクリアします。
*	すべての自動バインディングをクリアします。
<i>ip-address</i>	バインディング エントリ IP アドレスをクリアします。
interface <i>interface-id</i>	バインディング入力インターフェイスをクリアします。
vlan <i>vlan-id</i>	バインディング エントリ VLAN をクリアします。
database statistics	DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアします。
statistics	DHCP スヌーピング 統計カウンタをクリアします。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(37)SE	statistics キーワードが導入されました。
12.2(44)SE	*, <i>ip-address</i> 、 interface <i>interface-id</i> 、および vlan <i>vlan-id</i> キーワードが追加されました。

使用上のガイドライン

clear ip dhcp snooping database statistics コマンドを入力すると、スイッチは統計情報をクリアする前にバインディング データベースおよびバインディング ファイル内のエントリを更新しません。

例

次の例では、DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアする方法を示します。

```
Switch# clear ip dhcp snooping database statistics
```

統計情報がクリアされたかどうかを確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。

■ clear ip dhcp snooping

次の例では、DHCP スヌーピング統計カウンタをクリアする方法を示します。

```
Switch# clear ip dhcp snooping statistics
```

統計情報がクリアされたかどうかを確認するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping database	DHCP スヌーピング バインディング データベース エージェントまたはバインディング ファイルを設定します。
show ip dhcp snooping binding	DHCP スヌーピング データベース エージェントのステータスを表示します。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベース エージェントの統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を表示します。

clear lacp

Link Aggregation Control Protocol (LACP) チャンネル グループ カウンタをクリアするには、**clear lacp** 特権 EXEC コマンドを使用します。

```
clear lacp {channel-group-number counters | counters}
```

シンタックスの説明	<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 ~ 6 です。
	counters	トラフィックのカウンタをクリアします。

デフォルト デフォルトは定義されていません。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **clear lacp counters** コマンドを使用することで、カウンタをすべてクリアできます。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場合には、**clear lacp channel-group-number counters** コマンドを使用します。

例 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。

```
Switch# 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。

```
Switch# clear lacp 4 counters
```

情報が削除されたかどうかを確認するには、**show lacp counters** または **show lacp 4 counters** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show lacp	LACP チャンネル グループ情報を表示します。

clear mac address-table

MAC アドレス テーブルから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、または特定の VLAN 上のすべてのダイナミック アドレスを削除するには、**clear mac address-table** 特権 EXEC コマンドを使用します。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] | notification}
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
dynamic address <i>mac-addr</i>	(任意) 指定されたダイナミック MAC アドレスを削除します。
dynamic interface <i>interface-id</i>	(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 MAC アドレスを削除します。
dynamic vlan <i>vlan-id</i>	(任意) 指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ~ 4094 です。
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。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、ダイナミック アドレス テーブルから指定の MAC アドレスを削除する方法を示します。

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

情報が削除されたかどうかを確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

関連コマンド

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。
show mac access-group	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。

コマンド	説明
<code>show mac address-table notification</code>	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。
<code>snmp trap mac-notification</code>	特定のインターフェイス上の Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) MAC アドレス通知トラップをイネーブルにします。

clear mac address-table move update

MAC アドレス テーブルの移行更新に関連したカウンタをクリアするには、**clear mac address-table move update** 特権 EXEC コマンドを使用します。

clear mac address-table move update

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

例

次の例では、MAC アドレス テーブル移行更新関連カウンタをクリアする方法を示します。

```
Switch# clear mac address-table move update
```

情報がクリアされたかどうかを確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mac address-table move update {receive transmit}	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

clear nmsp statistics

Network Mobility Services Protocol (NMSP; ネットワーク モビリティ サービス プロトコル) 統計情報をクリアするには、**clear nmsp statistics** 特権 EXEC コマンドを使用します。このコマンドを使用できるのは、スイッチで暗号化ソフトウェア イメージが実行されている場合だけです。

clear nmsp statistics



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

例 次の例では、NMSP 統計情報をクリアする方法を示します。

```
Switch# clear nmsp statistics
```

情報が削除されたかどうかを確認するには、**show nmsp statistics** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show nmsp	NMSP 情報を表示します。

clear pagp

ポート集約プロトコル (PAgP) チャンネル グループ情報をクリアするには、**clear pagp** 特権 EXEC コマンドを使用します。

```
clear pagp {channel-group-number counters | counters}
```

シンタックスの説明

<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 ~ 6 です。
counters	トラフィックのカウンタをクリアします。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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、**clear pagp channel-group-number counters** コマンドを使用すると、指定のチャンネル グループのカウンタだけをクリアできます。

例

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。

```
Switch# 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。

```
Switch# clear pagp 10 counters
```

情報が削除されたかどうかを確認するには、**show pagp** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show pagp	PAgP チャンネル グループ情報を表示します。

clear port-security

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定タイプ（設定済み、ダイナミック、スティッキー）のすべてのセキュア アドレスを削除するには、**clear port-security** 特権 EXEC コマンドを使用します。

```
clear port-security {all | configured | dynamic | sticky} [[address mac-addr | interface
interface-id] [vlan {vlan-id | {access | voice}}]]
```

シンタックスの説明

all	すべてのセキュア MAC アドレスを削除します。
configured	設定済みセキュア MAC アドレスを削除します。
dynamic	ハードウェアによって自動学習されたセキュア MAC アドレスを削除します。
sticky	自動学習または設定済みセキュア 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 セキュア 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 VLAN 上のすべてのダイナミック セキュア MAC アドレスを削除します。
vlan	(任意) 指定された VLAN から指定されたセキュア MAC アドレスを削除します。 vlan キーワードを入力後、以下のいずれかのオプションを入力します。 <ul style="list-style-type: none"> vlan-id : トランク ポート上で、クリアする必要のあるアドレスの VLAN の VLAN ID を指定します。 access : アクセス ポートで、アクセス VLAN 上の指定されたセキュア MAC アドレスをクリアします。 voice : アクセス ポートで、音声 VLAN 上の指定されたセキュア MAC アドレスをクリアします。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合のみ利用可能です。</p>

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、MAC アドレス テーブルからすべてのセキュア アドレスを削除する方法を示します。

```
Switch# clear port-security all
```

■ clear port-security

次の例では、MAC アドレス テーブルから特定の設定済みセキュア アドレスを削除する方法を示します。

```
Switch# clear port-security configured address 0008.0070.0007
```

次の例では、特定のインターフェイスで学習されたすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

次の例では、アドレス テーブルからすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic
```

情報が削除されたかどうかを確認するには、**show port-security** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
switchport port-security	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します。
switchport port-security mac-address mac-address	セキュア MAC アドレスを設定します。
switchport port-security maximum value	セキュア インターフェイスにセキュア MAC アドレスの最大数を設定します。
show port-security	インターフェイスまたはスイッチに定義されたポート セキュリティ設定を表示します。

clear spanning-tree counters

スパニングツリー カウンタをクリアするには、**clear spanning-tree counters** 特権 EXEC コマンドを使用します。

clear spanning-tree counters [**interface** *interface-id*]

シンタックスの説明	interface <i>interface-id</i> (任意) 指定のインターフェイスのスパニングツリー カウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、およびポート チャネルがあります。指定できる VLAN 範囲は 1 ~ 4094 です。ポート チャネル範囲は 1 ~ 6 です。
-----------	--

デフォルト デフォルトは定義されていません。

コマンドモード 特権 EXEC

コマンドの履歴	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>12.2(25)FX</td><td>このコマンドが追加されました。</td></tr></tbody></table>	リリース	変更内容	12.2(25)FX	このコマンドが追加されました。
リリース	変更内容				
12.2(25)FX	このコマンドが追加されました。				

使用上のガイドライン *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。

例 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。
Switch# **clear spanning-tree counters**

関連コマンド	<table><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td>show spanning-tree</td><td>スパニングツリー ステート情報を表示します。</td></tr></tbody></table>	コマンド	説明	show spanning-tree	スパニングツリー ステート情報を表示します。
コマンド	説明				
show spanning-tree	スパニングツリー ステート情報を表示します。				

clear spanning-tree detected-protocols

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上でプロトコル移行プロセスを再開する（強制的に近接スイッチと再ネゴシエートする）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

clear spanning-tree detected-protocols [*interface interface-id*]

シンタックスの説明

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セスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、およびポート チャンネルがあります。指定できる VLAN 範囲は 1 ~ 4094 です。ポート チャンネル範囲は 1 ~ 6 です。
-------------------------------	---

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+) プロトコルまたは Multiple Spanning-Tree Protocol (MSTP) が稼動しているスイッチは、組み込みプロトコル移行メカニズムをサポートしているため、レガシー IEEE 802.1D スイッチと相互に動作できます。Rapid PVST+ スイッチまたは MSTP スイッチが、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 Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) を受信した場合は、そのポートで IEEE 802.1D BPDU だけを送信します。Multiple Spanning-Tree (MST) スイッチが、レガシー BPDU、別のリージョンに関連付けられた MST BPDU (バージョン 3)、または Rapid Spanning-Tree (RST; 高速スパンニングツリー) 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。

ただし、スイッチは、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。

例

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。

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet0/1
```

関連コマンド

コマンド	説明
show spanning-tree	スパニングツリー ステート情報を表示します。
spanning-tree link-type	デフォルト リンクタイプ設定を上書きし、スパニングツリーがフォワーディング ステートに高速移行できるようにします。

clear vmps statistics

VLAN Query Protocol (VQP) クライアントが保持する統計情報をクリアするには、**clear vmps statistics** 特権 EXEC コマンドを使用します。

clear vmps statistics

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、VLAN Membership Policy Server (VMPS; VLAN メンバシップ ポリシー サーバ) 統計情報をクリアする方法を示します。

```
Switch# clear vmps statistics
```

情報が削除されたかどうかを確認するには、**show vmps statistics** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vmps	VQP バージョン、再確認間隔、再試行回数、VMPS IP アドレス、および現在のサーバとプライマリ サーバを表示します。

clear vtp counters

VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) カウンタとプルーニング カウンタをクリアするには、**clear vtp counters** 特権 EXEC コマンドを使用します。

clear vtp counters

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトは定義されていません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

例 次の例では、VTP カウンタをクリアする方法を示します。

```
Switch# clear vtp counters
```

情報が削除されたかどうかを確認するには、**show vtp counters** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show vtp	VTP 管理ドメイン、ステータス、カウンタの一般情報を表示します。

cluster commander-address

このコマンドは、スタンドアロン クラスタ メンバー スイッチから入力する必要はありません。クラスタ コマンド スイッチは、メンバー スイッチがクラスタに加入した場合に MAC アドレスをこれらのクラスタ メンバー スイッチに自動的に割り当てます。クラスタ メンバー スイッチは、この情報および他のクラスタ情報を実行コンフィギュレーション ファイルに追加します。デバッグまたは回復手順の間だけスイッチをクラスタから削除する場合は、クラスタ メンバー スイッチ コンソール ポートからこのグローバル コンフィギュレーション コマンドの **no** 形式を使用します。

cluster commander-address *mac-address* [**member number name** *name*]

no cluster commander-address

シンタックスの説明

<i>mac-address</i>	クラスタ コマンド スイッチの MAC アドレス
member number	(任意) 設定されたクラスタ メンバー スイッチの番号。指定できる範囲は 0 ~ 15 です。
name name	(任意) 設定されたクラスタの名前 (最大 31 文字)

デフォルト

このスイッチはどのクラスタのメンバーでもありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でのみ使用できます。

各クラスタ メンバーは、クラスタ コマンド スイッチを 1 つしか持てません。

クラスタ メンバー スイッチは、*mac-address* パラメータによりシステム リロード中にクラスタ コマンド スイッチの ID を保持します。

特定のクラスタ メンバー スイッチで **no** 形式を入力すると、デバッグまたはリカバリ手順の間そのクラスタ メンバー スイッチをクラスタから削除できます。通常は、メンバーがクラスタ コマンド スイッチと通信ができなくなった場合にのみ、クラスタ メンバー スイッチ コンソール ポートからこのコマンドを入力することになります。通常のスイッチ構成では、クラスタ コマンド スイッチで **no cluster member n** グローバル コンフィギュレーション コマンドを入力することによってのみ、クラスタ メンバー スイッチを削除することを推奨します。

スタンバイ クラスタ コマンド スイッチがアクティブになった場合 (クラスタ コマンド スイッチになった場合)、このスイッチは **cluster commander-address** 行をその設定から削除します。

例

次の例では、実行中のクラスタ メンバーの設定から、その出力を一部示します。

```
Switch(config)# show running-configuration
```

<output truncated>

```
cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster
```

<output truncated>

次の例では、クラスタ メンバー コンソールでクラスタからメンバーを削除する方法を示します。

```
Switch # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no cluster commander-address
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
debug cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster discovery hop-count

候補スイッチの拡張検出用にホップカウントの制限を設定するには、クラスタ コマンド スイッチ上で **cluster discovery hop-count** 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。

cluster discovery hop-count *number*

no cluster discovery hop-count

シンタックスの説明

<i>number</i>	クラスタ コマンド スイッチが候補の検出を制限するクラスタ エッジからのホップの数。指定できる範囲は 1 ~ 7 です。
---------------	--

デフォルト

ホップ カウントは 3 に設定されています。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でのみ利用できます。このコマンドは、クラスタ メンバー スイッチでは機能しません。

ホップ カウントが 1 に設定された場合、拡張検出はディセーブルになります。クラスタ コマンド スイッチは、クラスタのエッジから 1 ホップの候補だけを検出します。クラスタのエッジとは、最後に検出されたクラスタのメンバー スイッチと最初に検出された候補スイッチの間の点です。

例

次の例では、ホップ カウント制限を 4 に設定する方法を示します。このコマンドは、クラスタ コマンド スイッチ上から実行します。

```
Switch(config)# cluster discovery hop-count 4
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	候補スイッチのリストを表示します。

cluster enable

このコマンド対応スイッチをクラスタ コマンド スイッチとしてイネーブルにし、クラスタ名を割り当て、任意でメンバー番号を割り当てるには、コマンド対応スイッチ上で **cluster 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。すべてのメンバーを削除して、このクラスタ コマンド スイッチを候補スイッチにするには、このコマンドの **no** 形式を使用します。

cluster enable name [command-switch-member-number]

no cluster enable

シンタックスの説明

<i>name</i>	クラスタ名 (最大 31 文字)。指定できる文字は、英数字、ダッシュ、および下線です。
<i>command-switch-member-number</i>	(任意) クラスタのクラスタ コマンド スイッチにメンバー番号を割り当てます。指定できる範囲は 0 ~ 15 です。

デフォルト

このスイッチはクラスタ コマンド スイッチではありません。
 クラスタ名は定義されません。
 スイッチがクラスタ コマンド スイッチである場合、メンバー番号は 0 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、どのクラスタにも属していない任意のコマンド対応スイッチ上で入力します。装置がすでにクラスタのメンバーとして設定されている場合、コマンドはエラーとなります。

クラスタ コマンド スイッチをイネーブルにするときには、クラスタに名前を付けてください。スイッチがすでにクラスタ コマンド スイッチとして設定されており、クラスタ名が以前の名前と異なっている場合、コマンドはクラスタ名を変更します。

例

次の例では、クラスタ コマンド スイッチをイネーブルにし、クラスタに名前を付け、クラスタ コマンド スイッチ メンバー番号を 4 に設定する方法を示します。

```
Switch(config)# cluster enable Engineering-IDF4 4
```

設定を確認するには、クラスタ コマンド スイッチで **show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster holdtime

スイッチ（コマンドまたはクラスタ メンバー スイッチ）が、他のスイッチのハートビート メッセージを受信しなくなってからそのスイッチのダウンを宣言するまでの期間を秒単位で設定するには、**cluster holdtime** 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。期間をデフォルト値に設定する場合は、このコマンドの **no** 形式を使用します。

cluster holdtime *holdtime-in-secs*

no cluster holdtime

シンタックスの説明	<i>holdtime-in-secs</i>	スイッチ（コマンドまたはクラスタ メンバー スイッチ）が、他のスイッチのダウンを宣言するまでの期間（秒）。指定できる範囲は 1 ～ 300 秒です。
------------------	-------------------------	--

デフォルト デフォルトのホールド時間は 80 秒です。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン クラスタ コマンド スイッチ上でのみ、このコマンドと **cluster timer** 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ください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバーに伝達します。

ホールドタイムは通常インターバル タイマー（**cluster timer**）の倍数として設定されます。たとえば、スイッチのダウンを宣言するまでには、「ホールドタイムをインターバルタイムで割った秒数」回のハートビート メッセージが連続して受信されなかったこととなります。

例 次の例では、クラスタ コマンド スイッチでインターバル タイマーおよびホールド タイム時間を変更する方法を示します。

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster member

クラスタに候補を追加するには、クラスタ コマンド スイッチ上で **cluster member** 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。メンバーをクラスタから削除するには、このコマンドの **no** 形式を使用します。

cluster member [*n*] **mac-address** *H.H.H* [**password** *enable-password*] [**vlan** *vlan-id*]

no cluster member *n*

シンタックスの説明

<i>n</i>	クラスタ メンバーを識別する番号。指定できる範囲は 0 ~ 15 です。
mac-address <i>H.H.H</i>	クラスタ メンバー スイッチの Media Access Control (MAC; メディア アクセス制御) アドレス (16 進数)
password <i>enable-password</i>	候補スイッチのパスワードをイネーブルにします。候補スイッチにパスワードがない場合、パスワードは必要ありません。
vlan <i>vlan-id</i>	(任意) クラスタ コマンド スイッチが候補をクラスタに追加するときに使用される VLAN ID。指定できる範囲は 1 ~ 4094 です。

デフォルト

新しくイネーブルになったクラスタ コマンド スイッチには、関連するクラスタ メンバーはありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、候補をクラスタに追加したり、メンバーをクラスタから削除したりする場合にクラスタ コマンド スイッチでのみ入力できます。このコマンドをクラスタ コマンド スイッチ以外のスイッチで入力すると、スイッチはコマンドを拒否し、エラー メッセージを表示します。

スイッチをクラスタから削除する場合はメンバー番号を入力してください。ただし、スイッチをクラスタに追加する場合には、メンバー番号を入力する必要はありません。クラスタ コマンド スイッチは、次に利用可能なメンバー番号を選択し、これをクラスタに加入しているスイッチに割り当てます。

候補スイッチがクラスタに加入した場合には、認証を行うためにそのスイッチのイネーブル パスワードを入力してください。パスワードは、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションには保存されません。候補スイッチがクラスタのメンバーになったあと、そのパスワードはクラスタ コマンド スイッチ パスワードと同じになります。

スイッチが、設定されたホスト名を持たない場合、クラスタ コマンド スイッチは、メンバー番号をクラスタ コマンド スイッチ ホスト名に追加し、これをクラスタ メンバー スイッチに割り当てます。

VLAN ID を指定していない場合、クラスタ コマンド スイッチは自動的に VLAN を選択し、候補をクラスタに追加します。

例

次の例では、スイッチをメンバー 2、MAC アドレス 00E0.1E00.2222、パスワード *key* としてクラスタに追加する方法を示しています。クラスタ コマンド `スイッチ` は、VLAN 3 を経由して候補をクラスタに追加します。

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

次の例では、MAC アドレス 00E0.1E00.3333 のスイッチをクラスタに追加する方法を示します。このスイッチにはパスワードはありません。クラスタ コマンド `スイッチ` は、次に利用可能なメンバー番号を選択し、これをクラスタに加入しているスイッチに割り当てます。

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

設定を確認するには、クラスタ コマンド `スイッチ` で `show cluster members` 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>show cluster</code>	スイッチが属するクラスタのステータスおよびサマリーを表示します。
<code>show cluster candidates</code>	候補スイッチのリストを表示します。
<code>show cluster members</code>	クラスタ メンバーに関する情報を表示します。

cluster outside-interface

クラスタの Network Address Translation (NAT; ネットワーク アドレス変換) の外部インターフェイスを設定し、IP アドレスのないメンバーがクラスタの外部にある装置と通信できるようにするには、**cluster outside-interface** 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。

cluster outside-interface *interface-id*

no cluster outside-interface

シンタックスの説明	<i>interface-id</i>	外部インターフェイスとして機能するインターフェイス。有効なインターフェイスとしては、物理インターフェイス、ポート チャネル、または VLAN があります。指定できるポート チャネル範囲は 1 ~ 6 です。指定できる VLAN 範囲は 1 ~ 4094 です。
------------------	---------------------	--

デフォルト デフォルトの外部インターフェイスは、クラスタ コマンド スイッチによって自動的に選択されます。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン このコマンドは、クラスタ コマンド スイッチ上でのみ入力できます。クラスタ メンバー スイッチで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。

例 次の例では、VLAN 1 に外部インターフェイスを設定する方法を示します。

```
Switch(config)# cluster outside-interface vlan 1
```

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。

関連コマンド	コマンド	説明
	show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。

cluster run

スイッチ上でクラスタリングをイネーブルにするには、**cluster run** 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。スイッチでクラスタ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。

cluster run

no cluster run

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべてのスイッチでクラスタリングがイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

クラスタ コマンド スイッチ上で **no cluster run** コマンドを入力すると、クラスタ コマンド スイッチはディセーブルになります。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタ メンバー スイッチで **no cluster run** コマンドを入力すると、このメンバー スイッチはクラスタから削除されます。クラスタリングはディセーブルになり、スイッチは候補スイッチになることができません。

クラスタに属していないスイッチで **no cluster run** コマンドを入力すると、クラスタリングはそのスイッチ上でディセーブルになります。このスイッチは候補スイッチになることができません。

例

次の例では、クラスタ コマンド スイッチでクラスタリングをディセーブルにする方法を示します。

```
Switch(config)# no cluster run
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

cluster standby-group

既存の Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) にクラスタをバインドしてクラスタ コマンド スイッチの冗長性をイネーブルにするには、**cluster standby-group** 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。**routing-redundancy** キーワードを入力することで、同一の HSRP グループが、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用できるようになります。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。

cluster standby-group *HSRP-group-name* [**routing-redundancy**]

no cluster standby-group

シンタックスの説明	
<i>HSRP-group-name</i>	クラスタにバインドされる HSRP グループの名前。設定できるグループ名は 32 文字までです。
routing-redundancy	(任意) 同一の HSRP スタンバイ グループをイネーブルにし、クラスタ コマンド スイッチの冗長性およびルーティングの冗長性に対して使用します。

デフォルト クラスタは、どの HSRP グループにもバインドされません。

コマンドモード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン このコマンドは、クラスタ コマンド スイッチ上でのみ入力できます。クラスタ メンバー スイッチでこれを入力すると、エラー メッセージが表示されます。

クラスタ コマンド スイッチは、クラスタ HSRP バインディング情報をすべてのクラスタ HSRP 対応メンバーに伝播します。各クラスタ メンバー スイッチはバインディング情報を NVRAM (不揮発性 RAM) に保存します。HSRP グループ名は、有効なスタンバイ グループである必要があります。そうでない場合、エラーが発生してコマンドが終了します。

クラスタにバインドする HSRP スタンバイ グループのすべてのメンバーに同じグループ名を使用する必要があります。バインドされる HSRP グループのすべてのクラスタ HSRP 対応メンバーに同じ HSRP グループ名を使用してください (クラスタを HSRP グループにバインドしない場合には、クラスタ コマンドおよびメンバーに異なる名前を使用できます)。

例 次の例では、*my_hsrp* という名前の HSRP グループをクラスタにバインドする方法を示します。このコマンドは、クラスタ コマンド スイッチ上から実行します。

```
Switch(config)# cluster standby-group my_hsrp
```

次の例では、同じ HSRP グループ名 *my_hsrp* を使用して、ルーティング冗長とクラスタ冗長を確立する方法を示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
```

cluster standby-group

次の例では、このコマンドがクラスタ コマンド スイッチから実行され、指定された HSRP スタンバイグループが存在しない場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp
%ERROR: Standby (my_hsrp) group does not exist
```

次の例では、このコマンドがクラスタ メンバー スイッチで実行された場合のエラー メッセージを示します。

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
%ERROR: This command runs on a cluster command switch
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。出力は、クラスタ内の冗長性がイネーブルになったかどうかを示します。

関連コマンド

コマンド	説明
standby ip	インターフェイスで HSRP をイネーブルにします。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show standby	スタンバイ グループ情報を表示します。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。

cluster timer

ハートビート メッセージの間隔を秒単位で設定するには、**cluster timer** 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。デフォルト値の間隔を設定する場合は、このコマンドの **no** 形式を使用します。

cluster timer *interval-in-secs*

no cluster timer

シンタックスの説明	<i>interval-in-secs</i>	ハートビート メッセージ間隔 (秒)。指定できる範囲は 1 ~ 300 秒です。
-----------	-------------------------	--

デフォルト	8 秒間隔です。
-------	----------

コマンド モード	グローバル コンフィギュレーション
----------	-------------------

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン	このコマンドと cluster holdtime グローバル コンフィギュレーション コマンドは、クラスタ コマンド スイッチ上でのみ入力してください。クラスタ内のすべてのスイッチ間で設定の一貫性が保たれるように、クラスタ コマンド スイッチはこの値をそのすべてのクラスタ メンバーに伝達します。
------------	---

ホールドタイムは通常ハートビート インターバル タイマー (**cluster timer**) の倍数として設定されます。たとえば、スイッチのダウンを宣言するまでには、「ホールドタイムをインターバル タイムで割った秒数」回のハートビート メッセージが連続して受信されなかったこととなります。

例	次の例では、クラスタ コマンド スイッチでハートビート間隔のタイマーおよび期間を変更する方法を示します。
---	--

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

設定を確認するには、**show cluster** 特権 EXEC コマンドを入力します。

■ cluster timer

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。

define interface-range

インターフェイス範囲マクロを作成するには、**define interface-range** 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。定義されたマクロを削除するには、このコマンドの **no** 形式を使用します。

define interface-range *macro-name interface-range*

no define interface-range *macro-name interface-range*

シンタックスの説明

<i>macro-name</i>	インターフェイス範囲マクロの名前（最大 32 文字）
<i>interface-range</i>	インターフェイス範囲。インターフェイス範囲の有効値については、「使用上の注意事項」を参照してください。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

マクロ名は、最大 32 文字の文字列です。

マクロには、最大 5 つの範囲を含めることができます。

ある範囲内のすべてのインターフェイスは同じタイプ、つまり、すべてがファストイーサネットポート、すべてがギガビットイーサネットポート、すべてが EtherChannel ポート、またはすべてが VLAN のいずれかでなければなりません。ただし、マクロ内では複数のインターフェイスタイプを組み合わせて行うことができます。

interface-range を入力する場合は、次のフォーマットを使用します。

- *type* {*first-interface*} - {*last-interface*}
- *interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。たとえば、**gigabitethernet 0/1 - 2** は有効な範囲指定ですが、**gigabitethernet 0/1-2** は有効な範囲指定ではありません。

type と *interface* の有効値は次のとおりです。

- **vlan** *vlan-id*、ここで、VLAN ID の範囲は 1 ~ 4094 です。



(注) コマンドラインインターフェイスには複数の VLAN ID を設定するオプションがありますが、サポートされていません。

■ define interface-range

VLAN インターフェイスは、**interface vlan** コマンドで設定してください (**show running-config** 特権 EXEC コマンドは、設定された VLAN インターフェイスを表示します)。**show running-config** コマンドで表示されない VLAN インターフェイスは、**interface-range** では使用できません。

- **port-channel** *port-channel-number*、ここで、*port-channel-number* は 1 ~ 6 です。
- **fastethernet** module/{*first port*} - {*last port*}
- **gigabitethernet** module/{*first port*} - {*last port*}

物理インターフェイス

- モジュールは常に 0 です。
- 有効な範囲は、*type 0/number - number* です (例 : **gigabitethernet 0/1 - 2**)。

範囲を定義するときは、ハイフン (-) の前にスペースが必要です。次に例を示します。

gigabitethernet0/1 - 2

複数の範囲を入力することもできます。複数の範囲を定義するときは、カンマ (,) の前の最初のエントリのあとにスペースが必要です。カンマのあとのスペースは任意になります。次に例を示します。

fastethernet0/3, gigabitethernet0/1 - 2

fastethernet0/3 -4, gigabitethernet0/1 - 2

例

次の例では、複数のインターフェイス マクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

関連コマンド

コマンド	説明
interface range	複数のポートで 1 つのコマンドを同時に実行します。
show running-config	定義されたマクロを含む現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。

delete

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除するには、**delete** 特権 EXEC コマンドを使用します。

```
delete [/force] [/recursive] filesystem:/file-url
```

シンタックスの説明	
/force	(任意) 削除を確認するプロンプトを抑制します。
/recursive	(任意) 指定されたディレクトリおよびそのディレクトリに含まれるすべてのサブディレクトリおよびファイルを削除します。
filesystem:	フラッシュ ファイル システムのエイリアスです。 ローカル フラッシュ ファイル システムの構文 flash:
/file-url	削除するパス (ディレクトリ) およびファイル名

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

/force キーワードを使用すると、削除プロセスにおいて削除の確認を要求するプロンプトが、最初の 1 回のみとなります。

/force キーワードを指定せずに **/recursive** キーワードを使用すると、ファイルごとに削除の確認を要求するプロンプトが表示されます。

プロンプト動作は、**file prompt** グローバル コンフィギュレーション コマンドの設定によって異なります。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。このコマンドの詳細については、『Cisco IOS Command Reference Release 12.1』を参照してください。

例

次の例では、新しいイメージのダウンロードが正常に終了したあとに、古いソフトウェア イメージを含むディレクトリを削除する方法を示します。

```
Switch# delete /force /recursive flash:/old-image
```

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:** 特権 EXEC コマンドを使用します。

■ delete

関連コマンド

コマンド	説明
archive download-sw	新しいイメージをスイッチにダウンロードし、既存のイメージを上書きまたは保存します。

deny (ARP アクセス リスト コンフィギュレーション)

DHCP バインディングと一致したアドレス解決プロトコル (ARP) パケットを拒否するには、**deny** ARP アクセス リスト コンフィギュレーション コマンドを使用します。指定したアクセス コントロール エントリ (ACE) をアクセス リストから削除する場合は、このコマンドの **no** 形式を使用します。

```
deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host
sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip
sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host
sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac
target-mac-mask}] [log]
```

```
no deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host
sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip
sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host
sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac
target-mac-mask}] [log]
```

シンタックスの説明

request	(任意) ARP 要求の照合条件を定義します。 request を指定しないと、すべての ARP パケットに対して照合が実行されます。
ip	送信元 IP アドレスを指定します。
any	任意の IP アドレスまたは MAC アドレスを拒否します。
host sender-ip	指定された送信元 IP アドレスを拒否します。
<i>sender-ip sender-ip-mask</i>	指定された範囲の送信元 IP アドレスを拒否します。
mac	送信元 MAC アドレスを拒否します。
host sender-mac	指定された送信元 MAC アドレスを拒否します。
<i>sender-mac sender-mac-mask</i>	指定された範囲の送信元 MAC アドレスを拒否します。
response ip	ARP 応答の IP アドレス値を定義します。
host target-ip	指定された宛先 IP アドレスを拒否します。
<i>target-ip target-ip-mask</i>	指定された範囲の宛先 IP アドレスを拒否します。
mac	ARP 応答の MAC アドレス値を拒否します。
host target-mac	指定された宛先 MAC アドレスを拒否します。
<i>target-mac target-mac-mask</i>	指定された範囲の宛先 MAC アドレスを拒否します。
log	(任意) ACE と一致したパケットをロギングします。

デフォルト

デフォルト値は設定されていません。ただし、ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。

コマンドモード

ARP アクセス リスト コンフィギュレーション

deny (ARP アクセス リスト コンフィギュレーション)

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

照合条件に基づいて ARP パケットを廃棄する deny 句を追加できます。

例

次の例では、ARP アクセス リストを定義し、IP アドレス 1.1.1.1 および MAC アドレス 0000.0000.abcd のホストからの ARP 要求と ARP 応答をいずれも拒否する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP アクセス コントロール リスト (ACL) を定義します。
ip arp inspection filter vlan	スタティック IP アドレスが設定されたホストからの ARP 要求と ARP 応答を許可します。
permit (ARP アクセス リスト コンフィギュレーション)	DHCP バインディングと一致した ARP パケットを許可します。
show arp access-list	ARP アクセス リストの詳細を表示します。

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、deny MAC アクセス リスト コンフィギュレーション コマンドを使用します。拒否条件を名前付き MAC アクセス リストから削除する場合は、このコマンドの **no** 形式を使用します。

```
{deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | cos cos | 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-idp]
```

```
no {deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | cos cos | 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-idp]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
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 マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP 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 マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP 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、Ethernet II または Subnetwork Access Protocol (SNAP) カプセル化を使用して、パケットのプロトコルを識別します。 <i>type</i> には、0 ~ 65535 の 16 進数を指定できます。 <i>mask</i> は、マッチングを行う前に EtherType に適用される <i>don't care</i> ビットのマスクです。
aarp	(任意) データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を選択します。
amber	(任意) EtherType DEC-Amber を選択します。
cos cos	(任意) プライオリティを設定するため、0 ~ 7 までの Class of Service (CoS; サービス クラス) 値を選択します。CoS に基づくフィルタリングは、ハードウェアでのみ実行可能です。 cos オプションが設定されているかどうかを確認する警告メッセージが表示されます。
dec-spanning	(任意) EtherType Digital Equipment Corporation (DEC) スパニング ツリーを選択します。
decnet-iv	(任意) EtherType DECnet Phase IV プロトコルを選択します。
diagnostic	(任意) EtherType DEC-Diagnostic を選択します。
dsm	(任意) EtherType DEC-DSM を選択します。
etype-6000	(任意) EtherType 0x6000 を選択します。
etype-8042	(任意) EtherType 0x8042 を選択します。

lat	(任意) EtherType DEC-LAT を選択します。
lavc-sca	(任意) EtherType DEC-LAVC-SCA を選択します。
lsap <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 <i>mask</i> は、マッチングを行う前に LSAP 番号に適用される <i>don't care</i> ビットのマスクです。
mop-console	(任意) EtherType DEC-MOP Remote Console を選択します。
mop-dump	(任意) EtherType DEC-MOP Dump を選択します。
msdos	(任意) EtherType DEC-MSDOS を選択します。
mumps	(任意) EtherType DEC-MUMPS を選択します。
netbios	(任意) EtherType DEC-Network Basic Input/Output System (NETBIOS) を選択します。
vines-echo	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) を選択します。
vines-ip	(任意) EtherType VINES IP を選択します。
xns-idp	(任意) 10 進数、16 進数、または 8 進数の任意の Ethertype である EtherType Xerox Network Systems (XNS) プロトコルスイート (0 ~ 65535) を選択します。



(注) **appletalk** は、コマンドラインのヘルプ スtringには表示されていますが、一致条件としてはサポートされていません。

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。表 2-4 に、Novell 用語と Cisco IOS 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一覧表示します。

表 2-4 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	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

デフォルト

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。

コマンドモード

MAC アクセス リスト コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。**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は、リストの末尾に暗黙的な **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。

名前付き MAC 拡張アクセス リストの詳細については、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。

例

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。

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

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。

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、EtherType 0x4321 のすべてのパケットを拒否します。

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

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。

関連コマンド

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 ベースのアクセス リストを作成します。
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 トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定された ACL を表示します。

dot1x

IEEE 802.1x 認証をグローバルにイネーブルにするには、**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。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 {critical {eapol | recovery delay milliseconds} | {guest-vlan supplicant} |
system-auth-control}
```

```
no dot1x {critical {eapol | recovery delay} | {guest-vlan supplicant} |
system-auth-control}
```



(注)

credentials name キーワードは、コマンドラインのヘルプ スtringには表示されますが、サポートされていません。

シンタックスの説明

critical {eapol recovery delay milliseconds}	アクセス不能な認証バイパス パラメータを設定します。詳細については、 dot1x critical (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。
guest-vlan supplicant	スイッチでオプションのゲスト VLAN の動作をグローバルにイネーブルにします。
system-auth-control	スイッチで IEEE 802.1x 認証をグローバルにイネーブルにします。

デフォルト

IEEE 802.1x 認証およびオプションのゲスト VLAN 動作がディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SEE	critical {eapol recovery delay milliseconds} キーワードが追加されました。

使用上のガイドライン

IEEE 802.1x 認証をグローバルにイネーブルにする前に、認証、認可、アカウントिंग (AAA) をイネーブルにし、認証方式リストを指定する必要があります。方式リストには、ユーザの認証に使用する、順序と認証方式が記述されています。

スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする前に、IEEE 802.1x 認証および EtherChannel が設定されているインターフェイスから EtherChannel の設定を削除します。

EAP-Transparent LAN Service (TLS) および EAP-MD5 で IEEE 802.1x を認証する Cisco Access Control Server (ACS) アプリケーションが稼動する装置を使用している場合、装置が ACS バージョン 3.2.1 以上で稼動していることを確認します。

スイッチでオプションの IEEE 802.1x ゲスト VLAN 動作をグローバルにイネーブルにするには、**guest-vlan supplicant** キーワードを使用することもできます。詳細については、**dot1x guest-vlan** コマンドを参照してください。

例 次の例では、スイッチで IEEE 802.1x 認証をグローバルにイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
```

次の例では、スイッチでオプションのゲスト VLAN 動作をグローバルにイネーブルにする方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical (グローバル コンフィギュレーション)	スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。
dot1x guest-vlan	アクティブ VLAN をイネーブルにし、IEEE 802.1x ゲスト VLAN として指定します。
dot1x port-control	ポートの許可ステータスの手動制御をイネーブルにします。
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x auth-fail max-attempts

ポートが制限 VLAN に移行するまで許容できる最大認証試行回数を設定するには、**dot1x auth-fail max-attempts** 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。

dot1x auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>max-attempts</i>	ポートが制限 VLAN に移行するまでに許容される最大の認証試行回数を指定します。指定できる範囲は 1 ~ 3 です。デフォルト値は 3 です。
---------------------	--

デフォルト

デフォルト値は 3 回です。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

VLAN で許容される最大の認証試行回数を再設定する場合、変更内容は再認証タイマーが期限切れになったあとで反映されます。

例

次の例では、ポート 3 の制限 VLAN にポートが移行する前に許容される最大の認証試行回数を 2 に設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>dot1x auth-fail vlan [vlan id]</code>	オプションの制限 VLAN の機能をイネーブルにします。
<code>dot1x max-reauth-req [count]</code>	ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する最大回数を設定します。
<code>show dot1x [interface interface-id]</code>	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x auth-fail vlan

ポート上で制限 VLAN をイネーブルにするには、**dot1x auth-fail vlan** 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。

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>vlan-id</i>	VLAN を 1 ~ 4094 の範囲で指定します。
----------------	----------------------------

デフォルト

制限 VLAN は設定されていません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

次のように設定されたポートで制限 VLAN を設定できます。

- シングルホスト (デフォルト) モード
- 認証用 auto モード

再認証をイネーブルにする必要があります。ディセーブルになっていると、制限 VLAN のポートは再認証要求を受け取りません。再認証プロセスを開始するには、制限 VLAN がポートからリンクダウン イベントまたは Extensible Authentication Protocol (EAP) ログオフ イベントを受け取る必要があります。ホストがハブを介して接続されている場合、ホストが切断されているとポートがリンクダウン イベントを受け取ることができず、次の再認証試行が行われるまで新しいホストが検出されないことがあります。

サブリカントが認証に失敗すると、ポートは制限 VLAN に移行し、EAP 認証成功メッセージがサブリカントに送信されます。サブリカントには実際の認証失敗が通知されないため、この制限ネットワークアクセスに混乱が生じることがあります。EAP の成功メッセージは、次の理由で送信されます。

- EAP の成功メッセージが送信されない場合、サブリカントは 60 秒ごと (デフォルト) に EAP 開始メッセージを送信して認証を行おうとします。
- 一部のホスト (たとえば、Windows XP を実行中のデバイス) は、EAP の成功メッセージを受け取るまで Dynamic Host Configuration Protocol (DHCP) を実行できません。

サブリカントは、認証から EAP 成功メッセージを受け取ったあとに不正なユーザ名とパスワードの組み合わせをキャッシュし、再認証のたびにその情報を使用する可能性があります。サブリカントが正しいユーザ名とパスワードの組み合わせを送信するまで、ポートは制限 VLAN のままになります。

レイヤ 3 ポートに使用する内部 VLAN は、制限 VLAN として設定することはできません。

VLAN を制限 VLAN と音声 VLAN の両方に設定することはできません。そのように設定すると、syslog メッセージが生成されます。

制限 VLAN ポートが無許可ステートに移行すると、認証プロセスが再起動されます。サブリカントが再度認証プロセスに失敗すると、認証は保持ステートで待機します。サブリカントが正常に再認証されたあと、すべての IEEE 802.1x ポートが再初期化され、通常の IEEE 802.1x ポートとして扱われます。

制限 VLAN を異なる VLAN として再設定すると、制限 VLAN のポートも移行し、そのポートは現在認証されたステートのままになります。

制限 VLAN をシャットダウンするか VLAN データベースから削除すると、制限 VLAN のポートはただちに無許可ステートに移行し、認証プロセスが再起動します。制限 VLAN 設定がまだ存在するため、認証は保持ステートで待機しません。制限 VLAN が非アクティブである間も、制限 VLAN がアクティブになったときにポートがただちに制限 VLAN になるように、すべての認証試行がカウントされます。

制限 VLAN は、シングルホストモード（デフォルトのポートモード）でのみサポートされます。このため、ポートが制限 VLAN に配置されると、サブリカントの MAC アドレスが MAC アドレス テーブルに追加され、ポートに表示される他の MAC アドレスがセキュリティ違反として扱われます。

例

次の例では、ポート 1 で制限 VLAN を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x auth-fail max-attempts [max-attempts]	サブリカントを制限 VLAN に割り当てる前に、試行可能な認証回数を設定します。
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x control-direction

Wake-on-LAN (WoL) 機能を搭載した IEEE 802.1x 認証をイネーブルにし、ポート制御を単一方向または双方向に設定するには、**dot1x control-direction** 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。

dot1x control-direction {both | in}

no dot1x control-direction



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

both	ポートの双方向制御をイネーブルにします。ポートは、ホストにパケットを送受信できません。
in	ポートの単一方向制御をイネーブルにします。ポートは、ホストにパケットを送信できますが、受信はできません。

デフォルト

ポートは双方向モードに設定されています。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

デフォルト設定の双方向モードに戻すには、このコマンドの **both** キーワードまたは **no** 形式を使用します。

WoL の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with Wake-on-LAN」を参照してください。

例

次の例では、単一方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction in
```

次の例では、双方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction both
```

設定を確認するには、**show dot1x all** 特権 EXEC コマンドを入力します。

show dot1x all 特権 EXEC コマンド出力は、ポート名とポートの状態を除き、すべてのスイッチで同一です。ホストがポートに接続されていてまだ認証されていない場合、次のように表示されます。

```
Supplicant MAC 0002.b39a.9275
```

```
AuthSM State = CONNECTING  
BendSM State = IDLE  
PortStatus = UNAUTHORIZED
```

dot1x control-direction in 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単一方向制御をイネーブルにする場合、これが **show dot1x all** コマンド出力で次のように表示されます。

```
ControlDirection = In
```

dot1x control-direction in 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も、設定の競合によりポートでこのモードをサポートできない場合、**show dot1x all** コマンド出力で次のように表示されます。

```
ControlDirection = In (Disabled due to port settings)
```

関連コマンド

コマンド	説明
show dot1x [all interface interface-id]	指定したインターフェイスに対する制御方向のポート設定ステータスを表示します。

dot1x credentials (グローバル コンフィギュレーション)

サブリカント スイッチのプロファイルを設定するには、**dot1x credentials** 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。

dot1x credentials profile

no dot1x credentials profile

シンタックスの説明	<i>profile</i>	サブリカント スイッチのプロファイルを指定します。
------------------	----------------	---------------------------

デフォルト	スイッチのプロファイルが設定されていません。
--------------	------------------------

コマンド モード	グローバル コンフィギュレーション
-----------------	-------------------

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン	このスイッチがサブリカントになるように別のスイッチをオーセンティケータとして設定する必要があります。
-------------------	--

例	次の例では、スイッチをサブリカントとして設定する方法を示します。 Switch(config)# dot1x credentials profile 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。
----------	---

関連コマンド	コマンド	説明
	cisp enable	Client Information Signalling Protocol (CISP) をイネーブルにします。
	show cisp	特定のインターフェイスの CISP 情報を表示します。

dot1x critical (グローバル コンフィギュレーション)

アクセス不能な認証バイパス機能 (クリティカル認証、または認証、認可、アカウントिंग [AAA] 失敗ポリシーと呼ばれることもあります) のパラメータを設定するには、**dot1x critical** 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。

```
dot1x critical {eapol | recovery delay milliseconds}
```

```
no dot1x critical {eapol | recovery delay}
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

eapol	スイッチによりクリティカルなポートが critical-authentication ステートに置かれた場合、EAPOL-Success メッセージを送信するようスイッチを指定します。
recovery delay milliseconds	リカバリ遅延期間 (ミリ秒) を指定します。指定できる範囲は 1 ~ 10000 ミリ秒です。

デフォルト

クリティカルなポートを **critical-authentication** ステートに置くことによって認証に成功した場合に、スイッチは EAPOL-Success メッセージをホストに送信しません。

リカバリ遅延期間は、1000 ミリ秒 (1 秒) です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

クリティカルなポートが **critical-authentication** ステートに置かれた場合、スイッチが EAPOL-Success メッセージを送信するよう指定するには、**eapol** キーワードを使用します。

使用不能な RADIUS サーバが使用可能になった場合にスイッチがクリティカルなポートを再初期化するために待機するリカバリ遅延期間を設定するには、**recovery delay milliseconds** キーワードを使用します。デフォルトのリカバリ遅延期間は 1000 ミリ秒です。ポートは、秒単位で再初期化できます。

アクセス不能な認証バイパスをポート上でイネーブルにするには、**dot1x critical** 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。スイッチがクリティカルなポートに割り当てるアクセス VLAN を設定するには、**dot1x critical vlan vlan-id** 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。

例

次の例では、リカバリ遅延期間として 200 をスイッチに設定する方法を示します。

■ dot1x critical (グローバル コンフィギュレーション)

```
Switch# dot1x critical recovery delay 200
```

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical (インターフェイス コンフィギュレーション)	アクセス不能な認証バイパス機能をイネーブルにし、この機能にアクセス VLAN を設定します。
show dot1x	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x critical (インターフェイス コンフィギュレーション)

アクセス不能な認証バイパス機能 (クリティカル認証、または認証、認可、アカウントिंग [AAA] 失敗ポリシーと呼ばれることもあります) をイネーブルにするには、**dot1x critical** インターフェイス 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。ポートが **critical-authentication** ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定することもできます。この機能をディセーブルにするか、または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。

dot1x critical [recovery action reinitialize | vlan *vlan-id*]

no dot1x critical [recovery | vlan]



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

recovery action reinitialize	アクセス不能な認証バイパスのリカバリ機能をイネーブルにし、認証サーバが使用可能になった場合にリカバリ アクションによりポートを認証するよう指定します。
vlan <i>vlan-id</i>	スイッチがクリティカルなポートに割り当てることのできるアクセス VLAN を指定します。指定できる範囲は 1 ~ 4094 です。

デフォルト

アクセス不能認証バイパス機能はディセーブルです。
リカバリ アクションは設定されていません。
アクセス VLAN は設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

ポートが **critical-authentication** ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を指定するには、**vlan *vlan-id*** キーワードを使用します。指定された VLAN タイプは、以下のポート タイプに適合している必要があります。

- クリティカルなポートがアクセス ポートの場合、VLAN はアクセス VLAN でなければなりません。
- クリティカルなポートがプライベート VLAN のホスト ポートである場合、VLAN はセカンダリプライベート VLAN でなければなりません。
- クリティカルなポートがルーテッド ポートの場合、VLAN を指定できます (指定は任意)。

■ dot1x critical (インターフェイス コンフィギュレーション)

クライアントで Windows XP を稼動し、クライアントが接続されているクリティカル ポートが critical-authentication ステートである場合、Windows XP はインターフェイスが認証されていないことを報告します。

Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。

アクセス不能認証バイパス機能および制限 VLAN を IEEE802.1x ポート上に設定できます。スイッチが制限付き VLAN でクリティカル ポートの再認証を試行し、RADIUS サーバがすべて使用できない場合、ポートの状態はクリティカル認証ステートに移行し、ポートは制限付き VLAN のままとなります。アクセス不能認証バイパス機能とポート セキュリティは、同じスイッチ ポートに設定できます。

例

次の例では、アクセス不能認証バイパス機能をポート 21 上でイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/21
Switch(config-if)# dot1x critical
Switch(config-if)# end
Switch(config)# end
Switch#
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x critical (グローバル コンフィギュレーション)	スイッチ上で、アクセス不能な認証バイパス機能のパラメータを設定します。
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x default

IEEE 802.1x パラメータをデフォルト値に戻すには、**dot1x default** 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 default

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト値は次のとおりです。

- ポート単位の IEEE 802.1x プロトコルのイネーブル ステータスはディセーブルです (force-authorized)。
- 再認証の試行間隔の秒数は 3600 秒です。
- 定期的な再認証はディセーブルです。
- 待機時間は 60 秒です。
- 再伝送時間は 30 秒です。
- 最高再伝送回数は 2 回です。
- ホスト モードはシングル ホストです。
- クライアントのタイムアウト時間は 30 秒です。
- 認証サーバのタイムアウト時間は 30 秒です。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、ポート上の IEEE 802.1x パラメータをリセットする方法を示します。

```
Switch(config-if)# dot1x default
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x fallback

クライアントが IEEE 802.1x 認証をサポートしていない場合のフォールバック方式として Web 認証を使用するようにポートを設定するには、**dot1xfallback** 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。

dot1x fallback profile

no dot1x fallback

シンタックスの説明	profile	IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイルを指定します。
-----------	---------	--

デフォルト フォールバックはイネーブルではありません。

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン このコマンドを入力する前に、スイッチで **dot1x port-control auto** 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必要があります。

例 次の例では、IEEE 802.1x 認証用に設定されているスイッチ ポートにフォールバック プロファイルを指定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。
	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。
	ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。

dot1x guest-vlan

アクティブな VLAN を IEEE 802.1x のゲスト VLAN として指定するには、**dot1x guest-vlan** 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。

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

シンタックスの説明

<i>vlan-id</i>	アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。
----------------	--

デフォルト

ゲスト VLAN は設定されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

次のいずれかのスイッチポートにゲスト VLAN を設定できます。

- 非プライベート VLAN に属するスタティックアクセス ポート
- セカンダリ プライベート VLAN に属するプライベート VLAN ポート。スイッチ ポートに接続されるすべてのホストは、端末状態の妥当性の評価に成功したかどうかにかかわらず、プライベート VLAN に割り当てられます。スイッチが、スイッチのプライマリおよびセカンダリ プライベート VLAN の対応付けを使用してプライマリ プライベート VLAN を判別します。

スイッチの IEEE 802.1x ポートごとにゲスト VLAN を設定して、現在 IEEE 802.1x 認証を実行していないクライアント（スイッチに接続されているデバイスまたはワークステーション）へのサービスを制限できます。こうしたユーザは IEEE 802.1x 認証のためにシステムをアップグレードできますが、Windows 98 システムなどのホストでは IEEE 802.1x に対応できません。

IEEE 802.1x ポートでゲスト VLAN をイネーブルにした場合、認証サーバが Extensible Authentication Protocol over LAN (EAPOL) Request/Identity フレームに対する応答を受信しないと、あるいは EAPOL パケットがクライアントから送信されないと、スイッチではクライアントをゲスト VLAN に割り当てます。

スイッチは、EAPOL パケット履歴を保持します。リンクの存続時間内に別の EAPOL パケットがインターフェイス上で検出された場合、ゲスト VLAN 機能はディセーブルになります。ポートがすでにゲスト VLAN ステートにある場合、ポートは無許可ステートに戻り、認証が再開されます。EAPOL 履歴はリンクの損失でリセットされます。

スイッチ ポートがゲスト VLAN に移行すると、IEEE 802.1x 非対応クライアントはいくつでもアクセスが許可されます。IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加入すると、ポートは RADIUS 設定 VLAN またはユーザ設定アクセス VLAN では無許可ステートに移行し、認証が再開されます。

ゲスト VLAN は、単一ホスト モードおよび複数ホスト モードの IEEE 802.1x ポート上でサポートされます。

リモート スイッチド ポート アナライザ (RSPAN) VLAN、音声 VLAN 以外のアクティブなすべての VLAN は、IEEE 802.1x のゲスト VLAN として設定できます。ゲスト VLAN の機能は、トランク ポート上ではサポートされません。サポートされるのはアクセス ポートのみです。

DHCP クライアントが接続されている IEEE 802.1x ポートのゲスト VLAN を設定したあと、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の IEEE 802.1x 認証プロセスを再起動する設定を変更できます。IEEE 802.1x 認証プロセスの設定を減らします (**dot1x timeout quiet-period** および **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド)。設定の減少量は、接続された IEEE 802.1x クライアントのタイプによって異なります。

Cisco IOS Release 12.2(25)SEE 以上では、スイッチは MAC 認証バイパスをサポートします。MAC 認証バイパスは IEEE 802.1x ポートでイネーブルの場合、スイッチは、EAPOL メッセージ交換を待機している間に IEEE802.1x 認証が期限切れになると、クライアントの MAC アドレスに基づいてクライアントを許可できます。スイッチは、IEEE 802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます (指定されていない場合)。詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication」の章の「Using IEEE 802.1x Authentication with MAC Authentication Bypass」を参照してください。

例

次の例では、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config-if)# dot1x guest-vlan 5
```

次の例では、スイッチの待機時間を 3 秒に設定し、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を 15 に設定する方法、および IEEE 802.1x ポートが DHCP クライアントに接続されているときに VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

次の例では、オプションのゲスト VLAN の動作をイネーブルにし、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x guest-vlan 5
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x	オプションのゲスト VLAN のサブリカント機能をイネーブルにします。
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x host-mode

IEEE 802.1x 許可ポート上で単一のホスト（クライアント）または複数のホストを許可するには、**dot1x host-mode** 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。IEEE 802.1x 許可ポート上で Multidomain Authentication (MDA; マルチドメイン認証) をイネーブルにするには、**multi-domain** キーワードを使用します。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 host-mode {multi-host | single-host | multi-domain}
```

```
no dot1x host-mode [multi-host | single-host | multi-domain]
```



(注)

multi-domain キーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。

シンタックスの説明

multi-host	スイッチ上で複数のホストをイネーブルにします。
single-host	スイッチ上で単一のホストをイネーブルにします。
multi-domain	スイッチ ポート上で MDA をイネーブルにします。

デフォルト

デフォルト設定は、single-host モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(46)SE1	multi-domain キーワードが追加されました。

使用上のガイドライン

このコマンドを使用すると、IEEE 802.1x 対応ポートを単一のクライアントに限定したり、複数のクライアントを IEEE 802.1x 対応ポートに接続したりすることができます。マルチホスト モードでは、接続されたホストのうち 1 つが許可されれば、すべてのホストのネットワーク アクセスが許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN [EAPOL]-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

ポート上で MDA をイネーブルにするには、**multi-domain** キーワードを使用します。MDA により、ポートがデータ ドメインと音声ドメインに振り分けられます。MDA では、同じ IEEE 802.1x 対応ポート上でデータ デバイスと IP Phone などの音声デバイス（Cisco 製または他社製）を同時に使用できません。

このコマンドを入力する前に、指定のポートに対して **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。

例

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにして、ポートの IEEE 802.1x 認証をイネーブルにし、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。

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

次の例では、IEEE 802.1x 認証をグローバルにイネーブルにする方法、IEEE 802.1x 認証をイネーブルにする方法、および指定のポート上で MDA をイネーブルにする方法を示します。

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x initialize

ポート上で新しく認証セッションを開始する前に、指定の IEEE 802.1x 対応ポートを無許可ステートに手動で戻すには、**dot1x initialize** 特権 EXEC コマンドを使用します。

dot1x initialize [interface interface-id]

シンタックスの説明	interface interface-id (任意) ポートを初期化します。
-----------	--

デフォルト	デフォルト設定はありません。
-------	----------------

コマンドモード	特権 EXEC
---------	---------

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン	<p>このコマンドは、IEEE 802.1x ステート マシンを初期化し、新たな認証環境を設定します。このコマンドを入力したあと、ポートの状態は無許可になります。</p> <p>このコマンドには、no 形式はありません。</p>
------------	---

例	<p>次の例では、ポートを手動で初期化する方法を示します。</p> <pre>Switch# dot1x initialize interface gigabitethernet0/22</pre> <p>ポートが無許可ステートになっていることを確認するには、show dot1x [interface interface-id] 特権 EXEC コマンドを入力します。</p>
---	--

関連コマンド	<table border="1"><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td>show dot1x [interface interface-id]</td><td>指定されたポートの IEEE 802.1x の状態を表示します。</td></tr></tbody></table>	コマンド	説明	show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。
コマンド	説明				
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。				

dot1x mac-auth-bypass

MAC 認証バイパス機能をイネーブルにするには、**dot1x mac-auth-bypass** 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。MAC 認証バイパ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。

dot1x mac-auth-bypass [eap | timeout inactivity value]

no dot1x mac-auth-bypass

シンタックスの説明

eap	(任意) 認証に Extensible Authentication Protocol (EAP) を使用するようスイッチを設定します。
timeout inactivity value	(任意) 接続されたホストが無許可ステートになる前に非アクティブである秒数を設定します。指定できる範囲は 1 ~ 65535 です。

デフォルト

MAC 認証バイパスはディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。
12.2(35)SE	timeout inactivity value キーワードが追加されました。

使用上のガイドライン

特に言及されないかぎり、MAC 認証バイパス機能の使用上のガイドラインは IEEE802.1x 認証の使用上のガイドラインと同じです。

ポートが MAC アドレスで認証されたあとで、ポートから MAC 認証バイパス機能をディセーブルにした場合、ポート ステートには影響ありません。

ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバデータベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。

ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが IEEE 802.1x 対応サブリカントであることを確認し、(MAC 認証バイパス機能ではなく) IEEE 802.1x 認証を使用してインターフェイスを認証します。

MAC 認証バイパスで認証されたクライアントは再認証できます。

MAC 認証バイパスと IEEE 802.1x 認証の相互作用の詳細については、ソフトウェア コンフィギュレーション ガイドの「Configuring IEEE 802.1x Port-Based Authentication」の章の「Understanding IEEE 802.1x Authentication with MAC Authentication Bypass」および「IEEE 802.1x Authentication Configuration Guidelines」を参照してください。

例 次の例では、MAC 認証バイパスをイネーブルにし、認証に EAP を使用するようスイッチを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass eap
```

次の例では、MAC 認証バイパスをイネーブルにし、接続されたホストが 30 秒間非アクティブである場合にタイムアウトを設定する方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass timeout inactivity 30
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x max-reauth-req

ポートが無許可ステートに変わるまでスイッチが認証プロセスを再起動する上限回数を設定するには、**dot1x max-reauth-req** 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。

dot1x max-reauth-req *count*

no dot1x max-reauth-req

シンタックスの説明

<i>count</i>	ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数です。指定できる範囲は 0 ~ 10 です。
--------------	--

デフォルト

デフォルトは 2 回です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	<i>count</i> 範囲が変更されました。

使用上のガイドライン

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。

例

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x max-req	スイッチが認証プロセスを再起動する前に、EAP フレームを認証サーバに送信する最高回数を設定します (応答を受信しないと仮定)。
dot1x timeout tx-period	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x max-req

認証プロセスを再起動するまでスイッチが Extensible Authentication Protocol (EAP) フレームを認証サーバからクライアントに送信する上限回数を設定するには (応答を受信しないと仮定)、**dot1x max-req** 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。

dot1x max-req count

no dot1x max-req

シンタックスの説明	<i>count</i>	スイッチが、認証プロセスを再起動する前に、認証サーバから EAP フレームを再送信する回数です。指定できる範囲は 1 ~ 10 です。
------------------	--------------	---

デフォルト デフォルトは 2 回です。

コマンド モード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン 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。

例 次の例では、認証プロセスを再起動する前に、スイッチが EAP フレームを認証サーバからクライアントに送信する回数を 5 回に設定する方法を示します。

```
Switch(config-if)# dot1x max-req 5
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	dot1x timeout tx-period	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。
	show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x pae

IEEE 802.1x Port Access Entity (PAE) オーセンティケータとしてポートを設定するには、**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。IEEE 802.1x 認証をポート上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。

dot1x pae authenticator

no dot1x pae

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートは IEEE 802.1x PAE オーセンティケータではありません。IEEE 802.1x 認証はポート上でディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

IEEE 802.1x 認証をポート上でディセーブルにする場合は、このコマンドの **no dot1x pae** 形式を使用します。

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、スイッチ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あとでディセーブルになります。

例

次の例では、ポートの IEEE 802.1x 認証をディセーブルにする方法を示します。

```
Switch(config-if)# no dot1x pae
```

設定を確認するには、**show dot1x** または **show eap** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x	スイッチ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します。
show eap	スイッチまたは特定のポートの EAP のレジストレーション情報およびセッション情報を表示します。

dot1x port-control

ポートの許可ステータスの手動制御をイネーブルにするには、**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 port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

シンタックスの説明

auto	ポートで IEEE 802.1x 認証をイネーブルにし、スイッチおよびクライアント間の IEEE 802.1x 認証交換に基づきポートを許可または無許可ステータスに変更します。
force-authorized	ポートで IEEE 802.1x 認証をディセーブルにすれば、認証情報の交換をせずに、ポートを許可ステータスに移行します。ポートはクライアントとの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
force-unauthorized	クライアントからの認証の試みをすべて無視し、ポートを強制的に無許可ステータスに変更することにより、このポート経由のすべてのアクセスを拒否します。スイッチはポートを介してクライアントに認証サービスを提供できません。

デフォルト

デフォルトの設定は **force-authorized** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

特定のポートの IEEE 802.1x 認証をイネーブルにする前に、**dot1x system-auth-control** 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、スイッチの IEEE 802.1x 認証をグローバルにイネーブルにする必要があります。

IEEE 802.1x 標準は、レイヤ 2 スタティック アクセス ポートと音声 VLAN ポートでサポートされません。

ポートが、次の項目の 1 つとして設定されていない場合に **auto** キーワードを使用することができます。

- **トランク ポート**：トランク 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 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、エラー メッセージが表示され、ポート モードは変更されません。
- **ダイナミック ポート**：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック 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。IEEE 802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。

- ダイナミック アクセス ポート：ダイナミック アクセス (VLAN Query Protocol [VQP]) ポートで IEEE 802.1x 認証をイネーブルにしようとすると、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。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。
- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバーを 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と、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。
- スイッチド ポート アナライザ (SPAN) およびリモート SPAN (RSPAN) 宛先ポート：SPAN または RSPAN 宛先ポートであるポートの IEEE 802.1x 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先として削除されるまで、IEEE 802.1x 認証はディセーブルのままです。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。

スイッチの IEEE 802.1x 認証をグローバルにディセーブルにするには、**no dot1x system-auth-control** 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。特定のポートの IEEE 802.1x 認証をディセーブルにするには、**no dot1x port-control** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポートの IEEE 802.1x 認証をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/21
Switch(config-if)# dot1x port-control auto
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x re-authenticate

指定の IEEE 802.1x 対応ポートの再認証を手動で開始するには、**dot1x re-authenticate** 特権 EXEC コマンドを使用します。

dot1x re-authenticate [*interface interface-id*]

シンタックスの説明	interface interface-id (任意) 再認証するインターフェイスのモジュールおよびポート番号
-----------	--

デフォルト	デフォルト設定はありません。
-------	----------------

コマンドモード	特権 EXEC
---------	---------

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン	このコマンドを使用すると、再認証試行間隔 (re-authperiod) および自動再認証の設定秒数を待たずにクライアントを再認証できます。
------------	--

例	次の例では、ポートに接続されたデバイスを手動で再認証する方法を示します。
---	--------------------------------------

```
Switch# dot1x re-authenticate interface gigabitethernet0/21
```

関連コマンド	コマンド	説明
	dot1x reauthentication	クライアントの定期的再認証をイネーブルにします。
	dot1x timeout reauth-period	再認証の間隔 (秒) を指定します。

dot1x reauthentication

クライアントの定期的な再認証をイネーブルにするには、**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 reauthentication

no dot1x reauthentication

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

定期的な再認証はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

dot1x timeout reauth-period インターフェイス コンフィギュレーション コマンドを使用して、定期的な再認証の試行間隔を設定します。

例

次の例では、クライアントの定期的な再認証をディセーブルにする方法を示します。

```
Switch(config-if)# no dot1x reauthentication
```

次の例では、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する方法を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x re-authenticate	すべての IEEE 802.1x 対応ポートの再認証を手動で初期化します。
dot1x timeout reauth-period	再認証の間隔 (秒) を指定します。
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

dot1x test eapol-capable

すべてのスイッチ ポート上の IEEE 802.1x アクティビティを監視し、IEEE 802.1x をサポートしているポートに接続されたデバイスに関する情報を表示するには、**dot1x test eapol-capable** 特権 EXEC コマンドを使用します。

dot1x test eapol-capable [*interface interface-id*]

シンタックスの説明	interface interface-id (任意) ポートを照会します。
-----------	---

デフォルト	デフォルト設定はありません。
-------	----------------

コマンドモード	特権 EXEC
---------	---------

コマンドの履歴	リリース	変更内容
	12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン	<p>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された装置の IEEE 802.1x 機能のテストを実行するには、このコマンドを使用します。</p> <p>このコマンドには、no 形式はありません。</p>
------------	--

例	<p>次の例では、スイッチ上の IEEE 802.1x 準備状態チェックをイネーブルにして、ポートを照会する方法を示します。この例では、接続された装置が IEEE 802.1x 対応であることを確認する（照会したポートから受け取った）応答も示します。</p>
---	---

```
switch# dot1x test eapol-capable interface gigabitethernet0/13
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet0/13 is EAPOL
capable
```

関連コマンド	<table border="1"> <thead> <tr> <th>コマンド</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>dot1x test timeout <i>timeout</i></td> <td>IEEE 802.1x 準備状態の照会で EAPOL 応答の待機に使用されるタイムアウトを設定します。</td> </tr> </tbody> </table>	コマンド	説明	dot1x test timeout <i>timeout</i>	IEEE 802.1x 準備状態の照会で EAPOL 応答の待機に使用されるタイムアウトを設定します。
コマンド	説明				
dot1x test timeout <i>timeout</i>	IEEE 802.1x 準備状態の照会で EAPOL 応答の待機に使用されるタイムアウトを設定します。				

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、**dot1x test timeout** 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。

dot1x test timeout *timeout*

シンタックスの説明	<i>timeout</i>	EAPOL 応答の待機時間 (秒単位)。指定できる範囲は 1 ~ 65535 秒です。
------------------	----------------	---

デフォルト デフォルト設定は 10 秒です。

コマンドモード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン EAPOL 応答の待機に使用す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。

例 次の例では、EAPOL 応答に 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。

```
Switch# dot1x test timeout 27
```

show run 特権 EXEC コマンドを入力すると、タイムアウト設定ステータスを確認できます。

関連コマンド	コマンド	説明
	dot1x test eapol-capable [interface interface-id]	すべてまたは指定した IEEE 802.1x 対応ポートに接続された装置の IEEE 802.1x 準備状態をチェックします。

dot1x timeout

IEEE 802.1x タイマーを設定するには、**dot1x timeout** 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。

```
dot1x timeout {quiet-period seconds | ratelimit-period seconds | reauth-period {seconds | server} | server-timeout seconds | supp-timeout seconds | tx-period seconds}
```

```
no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}
```

シンタックスの説明

quiet-period <i>seconds</i>	スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数。指定できる範囲は 1 ~ 65535 です。
ratelimit-period <i>seconds</i>	この期間中に認証に成功したクライアントからの Extensible Authentication Protocol over LAN (EAPOL) パケットをスイッチが無視した秒数 指定できる範囲は 1 ~ 65535 です。
reauth-period { <i>seconds</i> server }	再認証の間隔 (秒) を指定します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> seconds : 1 ~ 65535 の範囲で秒数を指定します。デフォルトは 3600 秒です。 server : セッションタイムアウト RADIUS 属性 (属性 [27]) の値として秒数を設定します。
server-timeout <i>seconds</i>	認証サーバに対して、スイッチの packets 再送信を待機する秒数。指定できる範囲は 30 ~ 65535 です。
supp-timeout <i>seconds</i>	スイッチが IEEE 802.1x クライアントへパケットを再送信する前に待機する秒数。指定できる範囲は 30 ~ 65535 です。
tx-period <i>seconds</i>	要求を再送信するまでスイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待機する秒数を設定します。指定できる範囲は 1 ~ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

reauth-period は 3600 秒です。

quiet-period は 60 秒です。

tx-period は 5 秒です。

supp-timeout は 30 秒です。

server-timeout は 30 秒です。

rate-limit は 1 秒です。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	tx-period キーワードの範囲が変更され、 reauth-period server キーワードが追加されました。
12.2(25)SEE	ratelimit-period キーワードが追加されました。
12.2(40)SE	tx-period seconds の範囲が間違っています。正しい範囲は 1 ~ 65535 です。

使用上のガイドライン

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だけの場合、**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、スイッチの動作に影響します。

待機時間の間、スイッチ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値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、スイッチ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。

例

次の例では、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する方法を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

次の例では、定期的な再認証をイネーブルにし、再認証の間隔としてセッションタイムアウト RADIUS 属性の値を指定する方法を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

次の例では、スイッチの待機時間を 30 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

次の例では、スイッチから認証サーバへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config)# dot1x timeout server-timeout 45
```

次の例では、EAP request フレームに対するスイッチからクライアントへの再送信時間を 45 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

次の例では、EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する方法を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

次の例では、認証に成功したクライアントからの EAPOL パケットをスイッチが無視する秒数を 30 と設定する方法を示します。

```
Switch(config-if)# dot1x timeout ratelimit-period 30
```

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x max-req	スイッチが、認証プロセスを再始動する前に、EAP-Request/Identity フレームを送信する最高回数を設定します。
dot1x reauthentication	クライアントの定期的再認証をイネーブルにします。
show dot1x	すべてのポートの IEEE 802.1x ステータスを表示します。

dot1x violation-mode

新しいデバイスがポートに接続された場合、またはすでに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そのポートに接続された場合に適用される違反モードを設定するには、**dot1x violation-mode** 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 violation-mode {shutdown | restrict | protect}

no dot1x violation-mode

シンタックスの説明

shutdown	予想されない新規の MAC アドレスが発生したポートまたは仮想ポートを errdisable にします。
restrict	違反エラーが発生したときに Syslog エラーを生成します。
protect	通知なしで新規の MAC アドレスからパケットを廃棄します。これは、デフォルト設定です。

デフォルト

デフォルトでは、**dot1x violation-mode protect** がイネーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

例

次の例では、IEEE 802.1x 対応ポートを errdisable として設定し、新しい装置がポートに接続されたときにシャットダウンする方法を示します。

```
Switch(config-if)# dot1x violation-mode shutdown
```

次の例では、新しい装置がポートに接続されるたびに、IEEE 802.1x 対応ポートがシステム エラーメッセージを生成し、ポートを制限モードに変更する方法を示します。

```
Switch(config-if)# dot1x violation-mode restrict
```

次の例では、新しい装置がポートに接続されるたびに無視するように、IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# dot1x violation-mode protect
```

設定を確認するには、**show dot1x [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。

duplex

ポートがデュプレックス モードで動作するように指定するには、**duplex** 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。ポー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。

duplex {auto | full | half}

no duplex

シンタックスの説明

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用のみ）。1000 または 10000 Mb/s で動作するインターフェイスに対して半二重モードを設定できません。

デフォルト

ファストイーサネットポートおよびギガビットイーサネットポートに対するデフォルトは **auto** です。

100BASE-x（-x は -BX、-FX、-FX-FE、または -LX）SFP モジュールのデフォルトは **full** です。

二重オプションは、1000BASE-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。

ご使用のスイッチでサポートされている SFP モジュールについては、製品のリリース ノートを参照してください。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファストイーサネットポートでは、接続されたデバイス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実行しない場合、ポートを **auto** に設定すると、**half** を指定するのと同じ効果があります。

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を自動ネゴシエートしないときにポートを **auto** に設定すると、**full** を指定する場合と同じ効果があります。



(注) 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どちらかに設定できます。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、スイッチはリンクの反対側の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実行できるのは、速度が **auto** に設定されている場合です。



注意

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、再度イネーブルになる場合があります。

スイッチの速度パラメータとデュプレックスパラメータの設定に関する注意事項については、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 Interface Characteristics」の章を参照してください。

例

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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# duplex full
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	スイッチのインターフェイスの設定を表示します。
speed	10/100 または 10/100/1000 Mb/s インターフェイスの速度を設定します。

energywise (グローバル コンフィギュレーション)

エンティティ上で EnergyWise をイネーブルにして設定するには、**energywise** 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。EnergyWise をディセーブルにして、EnergyWise の設定を解除する場合は、このコマンドの **no** 形式を使用します。

```
energywise {importance importance | keywords word,word,... | level level | management
udp-port-number | name name | neighbor [hostname] ip-address] udp-port-number | role role}
```

```
no energywise {importance | keywords | management | name | neighbor | role}
```

シンタックスの説明

importance <i>importance</i>	エンティティの重要度を設定します。 指定できる範囲は 1 ~ 100 です。
keywords <i>word,word,...</i>	エンティティに少なくとも 1 つのキーワードを割り当てます。 複数のキーワードを割り当てる場合は、各キーワードをカンマで区切りま す。キーワードの区切り文字としてスペースを使用しないでください。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入 れないでください。
level <i>level</i>	エンティティの電力レベルを設定します。 指定できる範囲は 1 ~ 10 です。
management <i>udp-port-number</i>	クエリーを送受信する UDP ポートを指定します。 指定できる範囲は 1 ~ 65000 です。
name <i>name</i>	EnergyWise に固有のエンティティ名を指定します。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入 れないでください。
neighbor [<i>hostname</i>] <i>ip-address</i>] <i>udp-port-number</i>	次のスタティック ネイバーを割り当てます。 <ul style="list-style-type: none"> (任意) ホスト名 (<i>hostname</i>) または IP アドレス (<i>ip-address</i>) クエリーを送受信する UDP ポート (<i>udp-port-number</i>) 指定できる範囲は 1 ~ 65000 です。
role <i>role</i>	EnergyWise ドメイン内のエンティティのロールを指定します (例 : lobby.b20)。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入 れないでください。

デフォルト

EnergyWise はディセーブルになっています。

importance は 1 に設定されています。

keywords は定義されていません。

level は 10 に設定されています。

energywise (グローバル コンフィギュレーション)

udp-port-number は 43440 に設定されています。

name はホスト名に設定されています。

neighbor は未割り当てになっています。

role はモデル番号に設定されています。

コマンドモード 特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ドメインにエンティティを追加すると、そのエンティティと PoE ポート上で EnergyWise がイネーブルになります。

例

次の例では、EnergyWise をイネーブルにする方法、ドメインにエンティティを割り当てる方法、およびパスワードを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
Switch(config)# energywise importance 50
Switch(config)# energywise keywords lab1,devlab
Switch(config)# energywise management 60500
Switch(config)# energywise name Entity01
Switch(config)# energywise neighbor TG3560G-21 43440
Switch(config)# energywise role role.labaccess
Switch(config)# end
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定とステータスを表示します。
show energywise domain	エンティティが属しているドメインを表示します。
show energywise recurrence	繰り返しの設定とステータスを表示します。

energywise (インターフェイス コンフィギュレーション)

Power over Ethernet (PoE) ポート上で EnergyWise を設定するには、**energywise** 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。EnergyWise をディセーブルにして、EnergyWise の設定を解除する場合は、このコマンドの **no** 形式を使用します。

energywise [**importance** *importance* | **keywords** *word,word,...* | **level** *level* [**recurrence at** *minute hour day_of_month month day_of_week*] | **name** *name* | **role** *role*]

no energywise [**importance** | **keywords** | **level** | **name** | **role**]

シンタックスの説明

importance <i>importance</i>	(任意) ポートの重要度を設定します。 指定できる範囲は 1 ~ 100 です。
keywords <i>word,word,...</i>	ポートに少なくとも 1 つのキーワードを割り当てます。 複数のキーワードを割り当てる場合は、各キーワードをカンマで区切ります。キーワードの区切り文字としてスペースを使用しないでください。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入れないでください。
level <i>level</i>	(任意) ポートの電力レベルを設定します。 指定できる範囲は 0 ~ 10 です。 電力レベルが 0 の場合は、ポートの電源が切断されています。 電力レベルが 1 ~ 10 の場合は、ポートの電源が投入されています。この範囲の値を入力すると、PoE ポートの電源を投入できます。
recurrence importance importance at minute hour day_of_month month day_of_week	(任意) 電源投入または電源切断の繰り返しを計画します。 <ul style="list-style-type: none"> importance importance : ドメイン内のポートの重要度を設定します。指定できる範囲は 1 ~ 100 です。 minute : 指定できる範囲は 0 ~ 59 です。* をワイルドカードとして使用します。 hour : 指定できる範囲は 0 ~ 23 です。* をワイルドカードとして使用します。 day_of_month : 指定できる範囲は 1 ~ 31 です。* をワイルドカードとして使用します。 month : 指定できる範囲は 1 (1月) ~ 12 (12月) です。* をワイルドカードとして使用します。 day_of_week : 指定できる範囲は 0 (日曜日) ~ 6 (土曜日) です。* をワイルドカードとして使用します。 <p>(注) 指定された時間は、PoE エンティティの時間帯に基づく現地時間になります。</p>

energywise (インターフェイス コンフィギュレーション)

name <i>name</i>	(任意) EnergyWise に固有のポート名を指定します。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入れないでください。
role <i>role</i>	(任意) ドメイン内のポートのロールを指定します (例: lobbyport)。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入れないでください。

デフォルト

importance は 1 に設定されています。

keywords は定義されていません。

level は 10 に設定されています。

name はポート名の短縮形に設定されています (例: Gigabit Ethernet 0/2 を表す Gi0.2)。

role はモデル番号に設定されています。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、PoE ポート上で EnergyWise をイネーブルにして設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# energywise level 10 recurrence importance 90 at 0 8 * * *
Switch(config-if)# energywise level 0 recurrence importance 90 at 0 20 * * *
Switch(config-if)# energywise importance 50
Switch(config-if)# energywise name lobbyInterface.3
Switch(config-if)# energywise role role.lobbyaccess
Switch(config-if)# end
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定とステータスを表示します。
show energywise domain	エンティティが属しているドメインを表示します。
show energywise recurrence	繰り返しの設定とステータスを表示します。

energywise domain

エンティティ上で EnergyWise をイネーブルにし、ドメインにエンティティを割り当て、ドメインのエンティティ間のセキュアな通信を確保するためにパスワードを設定するには、**energywise domain** 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。EnergyWise をディセーブルにして、EnergyWise の設定を解除する場合は、このコマンドの **no** 形式を使用します。

```
energywise domain domain-name secret [0 | 7] password [protocol udp port
udp-port-number [interface interface-id | ip ip-address]]
```

```
no energywise domain
```

シンタックスの説明	
domain <i>domain-name</i>	指定した <i>domain-name</i> のドメインにエンティティを割り当てます。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入れないでください。
secret [0 7] <i>password</i>	ドメインのエンティティ間のセキュアな通信を確保するために <i>password</i> を設定します。 <ul style="list-style-type: none"> (任意) 0 : 暗号化されていないパスワードを使用します。 (任意) 7 : 隠されたパスワードを使用します。 0 と 7 のいずれも入力しない場合は、エンティティでデフォルト値 0 が使用されます。 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入れないでください。
port <i>udp-port-number</i>	(任意) クエリーを送受信する UDP ポートを指定します。 指定できる範囲は 1 ~ 65000 です。
interface <i>interface-id</i>	(任意) EnergyWise メッセージの送信元のポートを指定します。
ip <i>ip-address</i>	(任意) EnergyWise メッセージの送信元の IP アドレスを指定します。

デフォルト

EnergyWise がディセーブルになっており、ドメインにエンティティが割り当てられていません。
password は設定されていません。
udp-port-number は 43440 に設定されています。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

energywise domain domain-name secret [0 | 7] password コマンドを入力すると、ネットワークおよび管理アプリケーションとの通信に最初に使用されるポートがエンティティで選択されます。

例

次の例では、EnergyWise をイネーブルにする方法、*domain-name* と *password* を設定する方法、および IP アドレスを指定する方法を示します。

```
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定とステータスを表示します。
show energywise domain	エンティティが属しているドメインを表示します。

energywise query

電力情報を表示したり、ドメイン内のエンティティまたは PoE ポートに電源を投入したりするには、**energywise query** 特権 EXEC コマンドを使用します。

```
energywise query importance importance {keywords word,word,... | name name} collect
{delta | usage}
```

```
energywise query importance importance {keywords word,word,... | name name} set level
level
```

```
energywise query importance importance {keywords word,word,... | name name} sum
{delta | usage}
```

シンタックスの説明

importance <i>importance</i>	importance の値を基準にして結果にフィルタを適用します。指定した値以下の値が割り当てられたエンティティだけが表示されます。 指定できる importance の範囲は 1 ~ 100 です。
keywords <i>word,word,...</i>	指定した 1 つまたは複数のキーワードを基準にして結果にフィルタを適用します。 複数のキーワードを指定する場合は、各キーワードをカンマで区切ります。キーワードの区切り文字としてスペースを使用しないでください。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入れないでください。
name <i>name</i>	名前を基準にして結果にフィルタを適用します。 ワイルドカードとして * を使用するか、 name 句の末尾にアスタリスクを指定します (name *)。 <ul style="list-style-type: none"> 英数字だけでなく、#、(、%、!、& などの記号も入力できます。 文字間、文字と記号間、記号間にアスタリスク (*) やスペースを入れないでください。
collect { delta usage }	エンティティまたは PoE ポートのデルタ/使用量の値を表示します。 <ul style="list-style-type: none"> delta : 現在の電力消費量と使用可能な電力量の差分を表示します。 usage : 現在の電力消費量のみを表示します。
set level <i>level</i>	エンティティまたは PoE ポートの電力レベルを設定します。 指定できる範囲は 0 ~ 10 です。 エンティティでサポートされているレベルは 1 ~ 10 です。 PoE ポートでサポートされているレベルは 0 ~ 10 です。
sum { delta usage }	エンティティまたは PoE ポートのデルタ/使用量の合計値を表示します。 <ul style="list-style-type: none"> delta : 現在の電力消費量と使用可能な電力量の差分の合計を表示します。 usage : 現在の電力消費量のみを表示します。

デフォルト

importance は 1 に設定されています。

level は 10 に設定されています。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

sum キーワードの結果に含まれる *Responded* 合計は正確ではありません。Queried 合計は正確であり、クエリーに応答したエンティティの合計数を表しています。

ポートの電源を投入または切断するには、**energywise query {keywords word,word,... | name name} set level level** コマンドを入力します。



注意

このクエリーはコマンドの入力対象のエンティティおよびクエリー条件に一致した他のドメイン デバイスに影響を及ぼすため、使用する際には十分に注意してください。

例

次の例では、エンティティ名を基準にフィルタを適用する方法を示します。

```
Switch# energywise query name phone* collect usage
EnergyWise query, timeout is 3 seconds:
```

Host	Name	Usage
2.2.2.21	phone	0.0 (W)
2.2.2.21	phone	15.4 (W)
2.2.2.21	phoneA	0.0 (W)
2.2.2.22	phone	0.0 (W)
2.2.2.21	phoneB	0.0 (W)
2.2.2.22	phoneC	15.4 (W)
2.2.2.21	phone	0.0 (W)
2.2.2.23	phoneD	15.4 (W)
2.2.2.21	phone	0.0 (W)

```
Queried: 9    Responded: 9    Time: 0.26 seconds
```

```
Switch# energywise query name * sum usage
EnergyWise query, timeout is 3 seconds:
```

```
Total Usage
-----
346.3 (W)
```

```
Queried: 147    Responded: 147    Time: 0.121 seconds
```

```
Switch# energywise query name lobby* collect usage

EnergyWise query, timeout is 3 seconds:

Host          Name          Usage
----          -
2.2.4.30      lobbyInterface.17 10.0 (W)

Queried: 1    Responded: 1    Time: 0.7 seconds
```

```
Switch# energywise query name Fa1.0.4* sum usage

EnergyWise query, timeout is 3 seconds:

Total Usage
-----
129.0 (W)

Queried: 10   Responded: 10   Time: 0.6 seconds
```

次の例では、デルタの合計値とドメイン内での考えられる電力変更を示します。

```
Switch# energywise query name * sum delta
EnergyWise query, timeout is 3 seconds:

Level  Label      Delta Power (W)
-----  -
0      Shut       -12.9
1      Hibernate  +723.8
2      Sleep      +723.8
3      Standby    +723.8
4      Ready      +723.8
5      Low        +723.8
6      Frugal     +723.8
7      Medium     +723.8
8      Reduced    +723.8
9      High       +723.8
10     Full       +723.8

Queried: 48   Responded: 48   Time: 0.15 seconds
```

次の例では、ドメイン内での電力消費量を示します。

```
Switch# show energywise children
Interface  Role          Name          Usage      Lvl  Imp  Type
-----  -
Gi0/1     control      SwitchA       86.0 (W)  10   100  parent
Gi0/1     interface    Gi0.1         0.0 (W)  10   20   child
.
.
.
Gi0/6     interface    Gi0.6         0.0 (W)  10   20   child
Gi0/7     role.lobbyaccess lobbyInterface.7 0.0 (W)  10   50   child
Gi0/8     interface    Gi0.8         0.0 (W)  10   20   child
<output truncated>
```

```
Switch# energywise query name * set level 0
EnergyWise query, timeout is 3 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
Success rate is (48/48) setting entities

Queried: 48   Responded: 48   Time: 0.996 seconds
```

```
Switch# energywise query name * set level 10
EnergyWise query, timeout is 3 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
Success rate is (48/48) setting entities

Queried: 48   Responded: 48   Time: 0.996 seconds
```

次の例では、キーワードを基準にして結果にフィルタを適用する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# energywise keywords lobby,sattelite
Switch(config-if)# energywise keywords public
Switch(config-if)# end
Switch# show running-config interface gigabitethernet0/2
!
interface GigabitEthernet0/2
 energywise level 0 recurrence importance 90 at 0 8 * * *
 energywise level 10 recurrence importance 90 at 0 20 * * *
 energywise importance 50
 energywise role role.lobbyaccess
 energywise keywords lobby,sattelite,public
 energywise name lobbyInterface.2
end
```

```
Switch# energywise query keyword lobby collect usage
EnergyWise query, timeout is 3 seconds:
```

Host	Name	Usage
2.2.4.30	lobbyInterface.17	15.4 (W)

```
Queried: 1   Responded: 1   Time: 0.0 seconds
```

```
Switch# energywise query keyword satellite sum usage
EnergyWise query, timeout is 3 seconds:
```

```
Total Usage
-----
15.4 (W)
```

```
Queried: 1   Responded: 1   Time: 0.11 seconds
```

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、**errdisable detect cause** 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。errdisable 検出機能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。

```
errdisable detect cause {all | bpduguard | dhcp-rate-limit | dtp-flap | gbic-invalid |
inline-power | link-flap | loopback | pagp-flap | security-violation shutdown vlan |
sfp-config-mismatch}
```

```
no errdisable detect cause {all | bpduguard | dhcp-rate-limit | dtp-flap | gbic-invalid |
inline-power | link-flap | loopback | pagp-flap | security-violation shutdown vlan |
sfp-config-mismatch}
```

BPDU ガード機能とポートセキュリティ機能では、このコマンドを使用すると、違反が発生した場合にポート全体をシャットダウンするのではなく、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グローバルに設定できます。

VLAN ごとに errdisable 機能をオフにしている BPDU ガード違反が発生した場合は、ポート全体がディセーブルになります。VLAN ごとに errdisable 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 bpduguard shutdown vlan
```

```
no errdisable detect cause bpduguard shutdown vlan
```

シンタックスの説明

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。
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	Dynamic Trunking Protocol (DTP; ダイナミック トランッキング プロトコル) 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 Gigabit Interface Converter (GBIC; ギガビット インターフェイス コンバータ) モジュールのエラー検出をイネーブルにします。 (注) このエラーは、スイッチ上の無効な Small Form-Factor Pluggable (SFP) モジュールを意味します。
inline-power	インライン パワーに対し、エラー検出をイネーブルにします。
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。
security-violation shutdown vlan	音声認識 802.1x セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致でエラー検出をイネーブルにします。

■ errdisable detect cause

コマンドのデフォルト

検出はすべての原因に対してイネーブルです。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設定されます (Per-VLAN errdisable の場合を除く)。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(37)SE	VLAN ごとのエラー検出機能が追加されました。 inline-power キーワードおよび sfp-config-mismatch キーワードが追加されました。
12.2(46)SE	security-violation shutdown vlan キーワードが追加されました。

使用上のガイドライン

原因 (**link-flap**、**dhcp-rate-limit** など) は、errdisable ステートが発生した理由です。原因がポートで検出された場合、ポートは 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、音声認識 802.1x セキュリティ、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 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。

原因に対して **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、ポートは 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、ポートを手動で errdisable ステートから回復させる必要があります。

例

次の例では、リンクフラップ errdisable 原因の errdisable 検出をイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの errdisable で BPDU ガードをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドは、音声認識 802.1x セキュリティを Per-VLAN errdisable に対してグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
<code>show errdisable detect</code>	errdisable 検出情報を表示します。
<code>show interfaces status err-disabled</code>	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。
<code>clear errdisable interface</code>	VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。

errdisable detect cause small-frame

着信 VLAN タグ付きパケットが小さいフレーム（67 バイト以下）であり、設定された最小レート（しきい値）で到着した場合にスイッチ ポートを **errdisable** にするには、**errdisable detect cause small-frame** 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。

errdisable detect cause small-frame

no errdisable detect cause small-frame

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

この機能は、ディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、小さいフレームの着信機能をグローバルにイネーブルにします。各ポートのしきい値を設定するには、**small violation-rate** 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。

errdisable recovery cause small-frame 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、ポートが自動的に再びイネーブルになるように設定できます。**errdisable recovery 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、回復時間を設定します。

例

次の例では、小さい着信フレームが設定されたしきい値で着信する場合に、スイッチ ポートを **errdisable** にする方法を示します。

```
Switch(config)# errdisable detect cause small-frame
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable recovery cause small-frame	復旧タイマーをイネーブルにします。
errdisable recovery interval interval	指定された errdisable ステートから回復する時間を指定します。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。
small violation-rate	小さい着信フレームによってポートが errdisable ステートになるレート（しきい値）を設定します。

errdisable recovery cause small-frame

小さいフレームの到着によって errdisable になったポートを自動的に再イネーブルにする回復タイマーをイネーブルにするには、スイッチ上で **errdisable recovery cause small-frame** 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。

errdisable recovery cause small-frame

no errdisable recovery cause small-frame

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

この機能は、ディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、errdisable ポートの回復タイマーをイネーブルにします。errdisable recovery interval *interval* 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、回復時間を設定します。

例

次の例では、回復タイマーを設定する方法を示します。

```
Switch(config)# errdisable recovery cause small-frame
```

設定を確認するには、**show interfaces** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable detect cause small-frame	着信フレームが設定された最小サイズより小さく、指定されたレート（しきい値）で着信する場合に、スイッチポートが errdisable ステートになるようにします。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。
small violation-rate	小さい着信フレームによってポートが errdisable ステートになるサイズを設定します。

errdisable recovery

回復メカニズム変数を設定するには、**errdisable recovery** グローバル コンフィギュレーション コマンドを設定します。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 | bpduguard | channel-misconfig | dhcp-rate-limit |
  dtp-flap | gbic-invalid | inline-power | link-flap | loopback | pagp-flap |
  psecure-violation | security-violation | sfp-mismatch | uddl | vmps} | {interval interval}}
```

```
no errdisable recovery {cause {all | bpduguard | channel-misconfig | dhcp-rate-limit |
  dtp-flap | gbic-invalid | inline-power | link-flap | loopback | pagp-flap |
  psecure-violation | security-violation | sfp-mismatch | uddl | vmps} | {interval interval}}
```

シンタックスの説明

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します。
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。
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 の設定矛盾による 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	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。 (注) 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	インライン パワーに対し、エラー検出をイネーブルにします。
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。
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。
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。
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-mismatch	SFP 設定の不一致でエラー検出をイネーブルにします。
uddl	UniDirectional Link Detection (UDLD; 単方向リンク検出) 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。

vmps	VLAN メンバシップ ポリシー サーバ (VMPS) 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。
interval interval	指定された errdisable ステートから回復する時間を指定します。指定できる範囲は 30 ~ 86400 秒です。すべての原因に同じ間隔が適用されます。デフォルト間隔は 300 秒です。 (注) errdisable recovery のタイマーは、設定された間隔値からランダムな差で初期化されます。実際のタイムアウト値と設定された値の差は、設定された間隔の 15% まで認められます。

デフォルト

すべての原因に対して回復はディセーブルです。
デフォルトの回復間隔は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(37)SE	VLAN ごとのエラー検出機能が追加されました。 inline-power キーワードおよび sfp-mismatch キーワードが追加されました。

使用上のガイドライン

原因 (**link-flap** や **bpduguard** など) は、errdisable ステートが発生した理由として定義されます。原因がポートで検出された場合、ポートは 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 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。

その原因に対して errdisable の回復をイネーブルにしない場合、ポートは、**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、ポートは 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、手動でポートを errdisable ステートから回復させる必要があります。

例

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。

```
Switch(config)# errdisable recovery cause bpduguard
```

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Switch(config)# errdisable recovery interval 500
```

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。

関連コマンド

コマンド	説明
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status err-disabled	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。
clear errdisable interface	VLAN ごとの errdisable 機能によって errdisable になったポートまたは VLAN から errdisable ステートをクリアします。

exception crashinfo

Cisco IOS イメージでエラーが発生した場合に拡張クラッシュ情報ファイルを作成するようにスイッチを設定するには、**exception crashinfo** 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。

exception crashinfo

no exception crashinfo

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチが拡張 crashinfo ファイルを作成します。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

基本 crashinfo ファイルには、失敗した Cisco IOS のイメージ名とバージョン、およびプロセッサレジスタのリストが含まれます。拡張 crashinfo ファイルには、スイッチの障害の原因を判別するのに役立つその他の追加情報が含まれます。

スイッチが拡張 crashinfo ファイルを作成しないように設定するには、**no exception crashinfo** 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。

例

次の例では、スイッチが拡張 crashinfo ファイルを作成しないように設定する方法を示します。

```
Switch(config)# no exception crashinfo
```

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。

関連コマンド

コマンド	説明
show running-config	定義されたマクロを含む現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

fallback profile

Web 認証のフォールバック プロファイルを作成するには、**fallback 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用しません。

fallback profile profile

no fallback profile

シンタックスの説明	profile	IEEE 802.1x 認証をサポートしていないクライアントのフォールバック プロファイルを指定します。
-----------	---------	--

デフォルト フォールバック プロファイルは設定されていません。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン フォールバック プロファイルは、サブリカントを持たない IEEE 802.1x ポートの IEEE 802.1x フォールバック動作を定義するために使用されます。サポートされる動作は、Web 認証へのフォールバックのみです。

fallback profile コマンドを入力すると、プロファイル コンフィギュレーション モードが開始され、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。

- **ip** : IP コンフィギュレーションを作成します。
- **access-group** : まだ認証されていないホストから送信されたパケットのアクセス コントロールを指定します。
- **admission** : IP アドミッション ルールを適用します。

例 次の例では、Web 認証で使用されるフォールバック プロファイルの作成方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

設定を確認するには、**show running-configuration [interface interface-id]** 特権 EXEC コマンドを入力します。

関連コマンド

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 メカニズムとして Web 認証を使用するようポートを設定します。
ip admission	スイッチ ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show dot1x [interface interface-id]	指定されたポートの IEEE 802.1x の状態を表示します。
show fallback profile	スイッチの設定済みプロファイルを表示します。

flowcontrol

インターフェイスの受信フロー制御ステートを設定するには、**flowcontrol** 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。ある装置に対して **send** が動作可能でオンになっていて、接続のもう一方の側で輻輳が検出された場合、休止フレームを送信することによって、リンクの相手側またはリモート装置に輻輳を通知します。ある装置に対してフロー制御 **receive** がオンで、休止フレームを受信した場合、データ パケットの送信は停止します。こうすることにより、輻輳期間中にデータ パケットの損失を防ぎます。

フロー制御をディセーブルにするには **receive off** キーワードを使用します。

flowcontrol receive {desired | off | on}



(注)

スイッチは、ポーズ フレームを受信できますが、送信はできません。

シンタックスの説明

receive	インターフェイスがリモート装置からフロー制御パケットを受信できるかどうかを設定します。
desired	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼働させることができます。
off	接続装置がフロー制御パケットをインターフェイスへ送信する機能をオフにします。
on	インターフェイスを、フロー制御パケットを送信する必要がある接続装置またはフロー制御パケットを送信する必要はないが送信することのできる接続装置とともに稼働させることができます。

デフォルト

デフォルトは、**flowcontrol receive off** に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このスイッチでは、送信フロー制御の休止フレームはサポートされません。

on および **desired** キーワードは同一の結果になることに注意してください。

flowcontrol コマンドを使用してポートが輻輳中にトラフィック レートを制御するよう設定する場合、フロー制御はポート上で次の条件のうちの 1 つに設定されます。

- **receive on** または **desired** : ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要のある接続済デバイスまたはポーズ フレームを送信できる接続済デバイスと連動できます。ポートはポーズ フレームを受信できます。
- **receive off** : フロー制御はどちらの方向にも動作しません。輻輳が生じて、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。

■ flowcontrol

表 2-5 は、各設定の組み合わせによるローカル ポートおよびリモート ポート上のフロー制御の結果を示したものです。表は **receive desired** キーワードの使用時と **receive on** キーワードの使用時の結果が同一になることを前提としています。

表 2-5 フロー制御設定およびローカル/リモート ポート フロー制御解決

フロー制御設定		フロー制御解決	
ローカル デバイス	リモート デバイス	ローカル デバイス	リモート デバイス
send off/receive on	send on/receive on	受信のみ行います。	送受信を行います。
	send on/receive off	受信のみ行います。	送信のみ行います。
	send desired/receive on	受信のみ行います。	送受信を行います。
	send desired/receive off	受信のみ行います。	送信のみ行います。
	send off/receive on	受信のみ行います。	受信のみ行います。
	send off/receive off	送受信を行いません。	送受信を行いません。
send off/receive off	send on/receive on	送受信を行いません。	送受信を行いません。
	send on/receive off	送受信を行いません。	送受信を行いません。
	send desired/receive on	送受信を行いません。	送受信を行いません。
	send desired/receive off	送受信を行いません。	送受信を行いません。
	send off/receive on	送受信を行いません。	送受信を行いません。
	send off/receive off	送受信を行いません。	送受信を行いません。

例

次の例では、リモート ポートによってフロー制御がサポートされないようにローカル ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/21
Switch(config-if)# flowcontrol receive off
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。

interface port-channel

ポートチャネルの論理インターフェイスへのアクセスまたは作成を行うには、**interface port-channel** 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。ポート チャネルを削除する場合は、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 *port-channel-number*

シンタックスの説明

port-channel-number ポート チャネル番号。指定できる範囲は 1 ～ 6 です。

デフォルト

ポート チャネル論理インターフェイスは定義されません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 EtherChannel では、物理ポートをチャネル グループに割り当てる前にポートチャネル 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、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。チャネル グループが最初の物理ポートを獲得すると、ポートチャネル インターフェイスは自動的に作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号を使用することもできれば、新しい番号を使用することもできます。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 チャネルを作成します。

チャネル グループ内の 1 つのポート チャネルだけが許可されます。

interface port-channel コマンドを使用する場合は、次の注意事項に従ってください。

- Cisco Discovery Protocol (CDP) を使用する場合には、これを物理ポートのみ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 メンバーであるポートを 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、そのポートは 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」を参照してください。

例

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。

```
Switch(config)# interface port-channel 5
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel channel-group-number detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
show etherchannel	チャンネルの EtherChannel 情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

interface range

インターフェイス レンジ コンフィギュレーション モードを開始し、複数のポート上でコマンドを同時に実行するには、**interface range** 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。インターフェイス範囲を削除する場合は、このコマンドの **no** 形式を使用します。

```
interface range {port-range | macro name}
```

```
no interface range {port-range | macro name}
```

シンタックスの説明	説明
<i>port-range</i>	ポート範囲。 <i>port-range</i> の有効値のリストについては、「使用上の注意事項」を参照してください。
<i>macro name</i>	マクロ名を指定します。

デフォルト このコマンドにはデフォルト設定はありません。

コマンドモード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン インターフェイス範囲を設定するモードを開始して入力した、すべてのインターフェイスのパラメータは、その範囲内のすべてのインターフェイスに対する属性になります。

VLAN については、既存の VLAN Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) でだけ **interface range** コマンドを使用することができます。VLAN の SVI を表示する場合は、**show running-config** 特権 EXEC コマンドを入力します。表示されない VLAN は、**interface range** コマンドで使用することはできません。**interface range** コマンドのもとで入力したコマンドは、この範囲のすべての既存の VLAN SVI に適用されます。

あるインターフェイス範囲に対して行われた設定変更は、すべて NVRAM に保存されますが、インターフェイス範囲自体は NVRAM に保存されません。

インターフェイス範囲は 2 つの方法で入力できます。

- 最大 5 つまでのインターフェイス範囲を指定。
- 定義済みのインターフェイス範囲マクロ設定を指定。

範囲内のすべてのインターフェイスは同じタイプ、つまり、すべてがファストイーサネットポート、すべてがギガビットイーサネットポート、すべてが EtherChannel ポート、またはすべてが VLAN のいずれかでなければなりません。ただし、各範囲をカンマ (,) で区切ることにより、1 つのコマンドで最大 5 つのインターフェイス範囲を定義できます。

port-range タイプおよびインターフェイスの有効値は次のとおりです。

- **vlan** *vlan-ID*。ここで、VLAN ID の範囲は 1 ~ 4094 です。



(注) 複数の VLAN を設定するオプションがコマンドライン インターフェイス (CLI) に表示されますが、サポートされていません。

- **fastethernet** *module*/*{first port} - {last port}*。ここで、*module* は常に 0 になります。
- **gigabitethernet** *module*/*{first port} - {last port}*。ここで、*module* は常に 0 になります。
物理インターフェイス
 - モジュールは常に 0 です。
 - 使用できる範囲は、*type0/number - number* です (例 : **gigabitethernet0/1 - 2**)。
- **port-channel** *port-channel-number - port-channel-number*、*port-channel-number* は 1 ~ 6 です。



(注) ポート チャンネルの **interface range** コマンドを使用した場合、範囲内の最初と最後のポート チャンネル番号はアクティブなポート チャンネルである必要があります。

範囲を定義するときは、最初の入力とハイフン (-) の間にスペースが必要です。

```
interface range gigabitethernet0/1 -2
```

複数の範囲を定義する場合は、カンマ (,) までの最初のエントリのあとにスペースを入れる必要があります。

```
interface range fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

同じコマンドでマクロとインターフェイス範囲の両方を指定することはできません。

また、*port-range* で単一インターフェイスを指定することもできます。つまりこのコマンドは、**interface interface-id** グローバル コンフィギュレーション コマンドに類似しています。

インターフェイスの範囲の設定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。

例

次の例では、**interface range** コマンドを使用して、インターフェイス範囲コンフィギュレーション モードを開始し、2 つのポートにコマンドを入力する方法を示します。

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

次の例では、同じ機能に対して 1 つのポート範囲マクロ *macro1* を使用方法を示します。この利点は、*macro1* を削除するまで再利用できることです。

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```


関連コマンド

コマンド	説明
define interface-range	インターフェイス範囲のマクロを作成します。
show running-config	スイッチで現在の動作設定情報を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

interface vlan

VLAN へのアクセスまたは作成を実行し、インターフェイス コンフィギュレーション モードを開始するには、**interface vlan** 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。VLAN を削除する場合は、このコマンドの **no** 形式を使用します。

```
interface vlan vlan-id
```

```
no interface vlan vlan-id
```

シンタックスの説明

<i>vlan-id</i>	VLAN 番号 指定できる範囲は 1 ~ 4094 です。
----------------	-------------------------------

デフォルト

デフォルトの VLAN インターフェイスは VLAN 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VLAN は、特定の VLAN に対して **interface vlan *vlan-id*** コマンドを初めて入力した場合に作成されます。*vlan-id* は、IEEE 802.1Q カプセル化トランクのデータ フレームに関連付けられた VLAN タグ、またはアクセス ポートに設定された VLAN ID に相当します。

no interface vlan *vlan-id* コマンドで VLAN を削除すると、削除されたインターフェイスはそれ以降 **show interfaces** 特権 EXEC コマンドの出力に表示されなくなります。



(注)

VLAN 1 インターフェイスを削除することはできません。

削除した VLAN は、削除したインターフェイスに対して **interface vlan *vlan-id*** コマンドを入力することで、元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

例

次の例では、VLAN ID 23 の新しい VLAN を作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

設定を確認するには、**show interfaces** および **show interfaces vlan *vlan-id*** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>show interfaces vlan <i>vlan-id</i></code>	すべてのインターフェイスまたは指定の VLAN の管理ステータスおよび動作ステータスを表示します。

ip access-group

レイヤ 2 インターフェイスへのアクセスを制御するには、**ip access-group** 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すべてまたは指定のアクセス 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。

ip access-group {*access-list-number* | *name*} {**in**}

no ip access-group [*access-list-number* | *name*] {**in**}

シンタックスの説明

<i>access-list-number</i>	IP アクセス コントロール リスト (ACL) の番号です。指定できる範囲は 1 ~ 199 または 1300 ~ 2699 です。
<i>name</i>	ip access-list 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 ACL 名です。
in	入力パケットに対するフィルタリングを指定します。

デフォルト

アクセス リストは、インターフェイスには適用されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

名前付きまたは番号付きの標準/拡張 IP アクセス リストをインターフェイスに適用できます。名前を付けてアクセス リストを定義するには、**ip access-list** 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。番号付きアクセス リストを定義するには、**access list** 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。1 ~ 99 および 1300 ~ 1999 の範囲の番号付き標準アクセス リスト、または 100 ~ 199 および 2000 ~ 2699 の範囲の番号付き拡張アクセス リストを使用できます。

このコマンドを使用して、アクセス リストをレイヤ 2 インターフェイスに適用できます。ただし、ポート ACL には、次のような制限があることに注意してください。

- ACL は受信方向に対してのみ適用できます。
- インターフェイスごとに 1 つの IP ACL と 1 つの MAC ACL のみを適用できます。
- Port ACL はロギングをサポートしていないため、IP ACL で **log** キーワードを指定しても無視されます。
- インターフェイスに適用された IP ACL は、IP パケットのみをフィルタにかけます。非 IP パケットをフィルタリングするには、MAC 拡張 ACL とともに **mac access-group** 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。

標準入力アクセス リストでは、スイッチは、パケットを受信すると、パケットの送信元アドレスをアクセス リストに比較して検査します。IP 拡張アクセス リストでは、任意で、宛先 IP アドレス、プロトコル タイプ、ポート番号などのパケット内の他のフィールドを検査することができます。アクセス リストがパケットを許可する場合に、スイッチはパケットの処理を続行します。アクセス リストがパケットを拒否する場合は、スイッチはそのパケットをドロップします。

指定したアクセス リストが存在しない場合は、すべてのパケットが通過します。

例 次の例では、ポートの入力パケットに IP アクセス リスト 101 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 101 in
```

設定を確認するには、**show ip interface**、**show access-lists**、または **show ip access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
access list	番号付き ACL を設定します。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。
ip access-list	名前付き ACL を設定します。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。
show access-lists	スイッチで設定された ACL を表示します。
show ip access-lists	スイッチで設定された IP ACL を表示します。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。
show ip interface	インターフェイスのステータスと設定に関する情報を表示します。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。

ip address

レイヤ 2 スイッチの IP アドレスを設定するには、**ip 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。IP アドレスを削除したり、IP 処理をディセーブルにしたりするには、このコマンドの **no** 形式を使用します。

ip address *ip-address subnet-mask* [**secondary**]

no ip address [*ip-address subnet-mask*] [**secondary**]

シンタックスの説明

<i>ip-address</i>	IP アドレス
<i>subnet-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。

デフォルト

IP アドレスは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

Telnet のセッションで、スイッチの IP アドレスを削除した場合、スイッチの接続が切断されます。ホストは、Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) Mask Request 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。ルータは、この要求に対して ICMP Mask Reply メッセージで応答します。

no ip address コマンドを使って IP アドレスを削除することで、特定のインターフェイス上の IP プロセスをディセーブルにできます。スイッチが、その IP アドレスのうちの 1 つを使用している他のホストを検出した場合、コンソールにエラー メッセージを送信します。

オプションで **secondary** キーワードを使用することで、セカンダリ アドレスの番号を無制限に指定することができます。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 ブロードキャストと ARP 要求は、IP ルーティング テーブル内のインターフェイス ルートと同様に、適切に処理されます。



(注)

ネットワーク セグメント上のすべてのルータがセカンダリの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。

スイッチが、Bootstrap Protocol (BOOTP) または Dynamic Host Configured Protocol (DHCP) サーバから IP アドレスを受信し、そのスイッチ IP アドレスを **no ip address** コマンドで削除した場合、IP 処理はディセーブルとなり、BOOTP サーバまたは DHCP サーバが再びアドレスを割り当てることはできません。

例

次の例では、サブネット ネットワークでレイヤ 2 スイッチの IP アドレスを設定する方法を示します。

```
Switch(config)# interface vlan 1  
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

ip admission

Web 認証をイネーブルにするには、**ip admission** 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。このコマンドは、**fallback-profile** モードでも使用できます。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



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>rule</i>	IP アドミッション ルールをインターフェイスに適用します。
-------------	--------------------------------

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

ip admission コマンドにより、スイッチ ポートに Web 認証ルールが適用されます。

例

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。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip admission rule1
```

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。

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config)# ip admission name rule1
Switch(config)# end
```

関連コマンド

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 メカニズムとして Web 認証を使用するようポートを設定します。
fallback profile	ポートで Web 認証をイネーブルにします。

コマンド	説明
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show ip admission	Network Admission Control (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。 詳細については、Cisco.com で『 <i>Network Admission Control Software Configuration Guide</i> 』を参照してください。

ip admission name proxy http

Web 認証をイネーブルにするには、**ip admission name proxy http** 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。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 proxy http

no ip admission name proxy http



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Web 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(35)SE	このコマンドが追加されました。

使用上のガイドライン

ip admission name proxy http コマンドにより、Web 認証がスイッチ上でグローバルにイネーブルになります。

スイッチ上で Web 認証をグローバルに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。

例

次の例では、スイッチポートで Web 認証のみを設定する方法を示します。

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config) # interface gigabitethernet0/1
Switch(config-if) # ip access-group 101 in
Switch(config-if) # ip admission rule
Switch(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。

```
Switch# configure terminal
Switch(config) # ip admission name rule2 proxy http
Switch(config) # fallback profile profile1
Switch(config) # ip access group 101 in
Switch(config) # ip admission name rule2
Switch(config) # interface gigabitethernet0/1
```

```
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

関連コマンド

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 メカニズムとして 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。
show ip admission	Network Admission Control (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。詳細については、Cisco.com で『 Network Admission Control Software Configuration Guide 』を参照してください。

ip arp inspection filter vlan

ダイナミック アドレス解決プロトコル (ARP) インスペクションがイネーブルの場合にスタティック IP アドレスが設定されたホストからの ARP 要求と ARP 応答を許可または拒否するには、**ip arp inspection filter vlan** 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 arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

no ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

シンタックスの説明

<i>arp-acl-name</i>	ARP アクセス コントロール リスト (ACL) の名前を指定します。
<i>vlan-range</i>	VLAN の番号または範囲を指定します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
static	(任意) static を指定すると、ARP ACL 内の暗黙的な deny 文が明示的な deny 文として扱われ、ACL に含まれているどの句にも一致しないパケットが廃棄されます。DHCP バインディングは使用されません。 このキーワードを指定しないと、パケットを拒否する明示的な deny 文が ACL 内に存在しなくなるため、ACL に含まれているどの句にも一致しないパケットを許可するか拒否するかが DHCP バインディングによって決定されます。

デフォルト

VLAN に適用される ARP ACL が定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ダイナミック ARP インスペクションを実行するために ARP ACL を VLAN に適用すると、IP-to-MAC アドレス バインディングを含む ARP パケットだけが ACL と比較されます。パケットが ACL で許可されると、スイッチはそのパケットを転送します。それ以外のタイプのパケットはすべて検証なしで入力 VLAN でブリッジングされます。

ACL 内の明示的な **deny** 文によってパケットがスイッチで拒否された場合、そのパケットは廃棄されません。暗黙的な **deny** 文によってパケットがスイッチで拒否された場合、そのパケットは DHCP バインディングのリストと比較されます (ただし、ACL がスタティックの場合を除きます。この場合は、パケットがバインディングと比較されません)。

ARP ACL を定義するか、または事前に定義されたリストの末尾に句を追加するには、**arp access-list acl-name** 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。

例 次の例では、ダイナミック ARP インスペクションを実行するために ARP ACL *static-hosts* を VLAN 1 に適用する方法を示します。

```
Switch(config)# ip arp inspection filter static-hosts vlan 1
```

設定を確認するには、**show ip arp inspection vlan 1** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
deny (ARP アクセスリスト コンフィギュレーション)	DHCP バインディングと一致した ARP パケットを拒否します。
permit (ARP アクセスリスト コンフィギュレーション)	DHCP バインディングと一致した ARP パケットを許可します。
show arp access-list	ARP アクセスリストの詳細を表示します。
show inventory vlan vlan-range	指定された VLAN に対するダイナミック ARP インスペクションの設定と動作ステータスを表示します。

ip arp inspection limit

インターフェイス上での着信アドレス解決プロトコル (ARP) 要求および応答のレートを制限するには、**ip arp inspection limit** 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。これにより、サービス拒絶攻撃が発生した場合にダイナミック ARP インспекションにすべてのスイッチ リソースが使用される点が回避されます。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 arp inspection limit {rate pps [burst interval seconds] | none}
```

```
no ip arp inspection limit
```

シンタックスの説明

rate pps	1 秒間に処理される着信パケット数の上限を指定します。指定できる範囲は 0 ~ 2048 Packets Per Second (pps; パケット/秒) です。
burst interval seconds	(任意) レートの高い ARP パケットの有無についてインターフェイスが監視される間隔 (秒) を指定します。指定できる範囲は 1 ~ 15 秒です。
none	この値を指定すると、処理できる着信 ARP パケットのレートの上限が設定されません。

デフォルト

このレートは、信頼できないインターフェイス上で 15 pps に設定されています。ただし、1 台のホストが 1 秒間に 15 台の新規ホストに接続できるスイッチド ネットワークであると仮定しています。

このレートは、信頼できるすべてのインターフェイス上で無制限になっています。

burst interval は 1 秒に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

このレートは、信頼できるインターフェイスと信頼できないインターフェイスのいずれにも適用されます。ダイナミック ARP インспекションに対応した複数の VLAN 間のパケットを処理できるようにトランク上で適切なレートを設定するか、または **none** キーワードを使用してレートを無制限にします。

いくつかのバースト期間にわたって設定された 1 秒間のレートを超えるパケットをスイッチが連続して受信すると、インターフェイスが **errdisable** ステートになります。

インターフェイスに対してレート制限を明示的に設定しないかぎり、インターフェイスの信頼状態を変更すると、レート制限もその信頼状態のデフォルト値に変更されます。レート制限を設定すると、インターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。**no ip arp inspection limit** 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、インターフェイスはそのデフォルト レート制限に戻されます。

集約を反映するためにトランク ポートのレートを高く設定する必要があります。着信パケットのレートがユーザ設定のレートを超えると、スイッチはインターフェイスを **errdisable** ステートにします。**errdisable** 回復機能により、回復設定に従ってポートが **errdisable** ステートから自動的に解除されます。

EtherChannel ポート上での着信 ARP パケットのレートは、すべてのチャネル メンバーからの着信 ARP パケットのレートの合計と同じになります。EtherChannel ポートのレート制限は、必ずすべてのチャネル メンバーの着信 ARP パケットのレートを調べてから設定してください。

例

次の例では、ポート上で着信 ARP 要求のレートを 25 pps に制限する方法とインターフェイス監視間隔を 5 秒に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection limit rate 25 burst interval 5
```

設定を確認するには、**show ip arp inspection interfaces interface-id** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show inventory interfaces	指定されたインターフェイスまたはすべてのインターフェイスに関して信頼状態と ARP パケットのレート制限を表示します。

ip arp inspection log-buffer

ダイナミック アドレス解決プロトコル (ARP) インスペクションのロギング バッファを設定するには、**ip arp inspection log-buffer** 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 arp inspection log-buffer {*entries number* | *logs number interval seconds*}

no ip arp inspection log-buffer {*entries* | *logs*}

シンタックスの説明

entries number	バッファにロギングされるエントリの数を指定します。指定できる範囲は 0 ~ 1024 です。
logs number interval seconds	指定されたシステム メッセージ生成間隔に必要なエントリの数を指定します。 logs number に指定できる範囲は 0 ~ 1024 です。値を 0 に設定すると、エントリはログ バッファに配置されますが、システム メッセージが生成されません。 interval seconds に指定できる範囲は 0 ~ 86400 秒 (1 日) です。値を 0 に設定すると、システム メッセージがただちに生成されず (ログ バッファは常に空になります)。

デフォルト

ダイナミック ARP インスペクションをイネーブルにした場合は、拒否または廃棄された ARP パケットがロギングされます。

ログ エントリの数は 32 に設定されています。

システム メッセージの数は 1 秒あたり 5 つに制限されています。

ロギング レート間隔は 1 秒に設定されています。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

logs キーワードと **interval** キーワードのいずれにも値 0 は使用できません。

logs と **interval** の設定は相互に関連しています。**logs number X** が **interval seconds Y** より大きい場合は、X を Y で割って (X/Y) 求められたシステム メッセージ数が 1 秒間に送信されます。それ以外の場合は、Y を X で割って (Y/X) 求められた間隔 (秒) で 1 つのシステム メッセージが送信されます。たとえば、**logs number** が 20、**interval seconds** が 4 の場合は、ログ バッファにエントリが存在するかぎり、スイッチから 1 秒間に 5 エントリ分のシステム メッセージが生成されます。

1 つのログ バッファ エントリは複数のパケットを表す場合があります。たとえば、インターフェイスが同じ ARP パラメータを使用して同じ VLAN 上で多数のパケットを受信した場合、スイッチはこれらのパケットを組み合わせて 1 つのエントリとしてログ バッファに格納し、システム メッセージを 1 つのエントリとして生成します。

ログバッファのオーバーフローが発生すると、ログイベントがログバッファと整合しなくなり、**show ip arp inspection log** 特権 EXEC コマンドの出力表示に影響が及びます。出力表示で、パケット数と時刻を除くすべてのデータが -- と表示されます。このエントリに関してそれ以外の統計情報は表示されません。このエントリに関する情報が表示されるようにするには、ログバッファ内のエントリの数を増やすか、またはロギングレートを高くします。

例 次の例では、エントリを 45 個まで保持できるようにログバッファを設定する方法を示します。

```
Switch(config)# ip arp inspection log-buffer entries 45
```

次の例では、ロギングレートを 4 秒あたり 20 ログエントリに設定する方法を示します。この設定では、ログバッファにエントリが存在する間は、スイッチから 1 秒間に 5 エントリ分のシステムメッセージが生成されます。

```
Switch(config)# ip arp inspection log-buffer logs 20 interval 4
```

設定を確認するには、**show ip arp inspection log** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP アクセス コントロール リスト (ACL) を定義します。
clear ip arp inspection log	ダイナミック ARP インспекションのログバッファをクリアします。
ip arp inspection vlan logging	VLAN ごとにロギングされるパケットのタイプを制御します。
show inventory log	ダイナミック ARP インспекション ログバッファの設定と内容を表示します。

ip arp inspection trust

どの着信アドレス解決プロトコル (ARP) パケットがインスペクションの対象となるかを判断できるインターフェイスの信頼状態を設定するには、**ip arp inspection 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。デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

ip arp inspection trust

no ip arp inspection trust

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

インターフェイスは、信頼できないインターフェイスです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチは信頼できるインターフェイス上で ARP パケットを受信すると、インスペクションなしでそのパケットを転送します。

信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP-to-MAC アドレス バインディングを持つかどうかを検証します。スイッチは無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドに指定されたロギング設定に従ってログ バッファにロギングします。

例

次の例では、信頼できるポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

設定を確認するには、**show ip arp inspection interfaces interface-id** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip arp inspection log-buffer	ダイナミック ARP インспекションのログ バッファを設定します。
show inventory interfaces	指定されたインターフェイスまたはすべてのインターフェイスに関して信頼状態と ARP パケットのレート制限を表示します。
show inventory log	ダイナミック ARP インспекション ログ バッファの設定と内容を表示します。

ip arp inspection validate

ダイナミック アドレス解決プロトコル (ARP) インスペクションに固有の検証を実行するには、**ip arp inspection validate** 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 arp inspection validate {[src-mac] [dst-mac] [ip [allow zeros] ]}
```

```
no ip arp inspection validate [src-mac] [dst-mac] [ip [allow zeros] ]
```

シンタックスの説明

src-mac	イーサネット ヘッダーの送信元 MAC アドレスを ARP 本文の送信元 MAC アドレスと比較します。この検証は、ARP 要求と ARP 応答に両方に対して実行されます。 イネーブルの場合、異なる MAC アドレスが割り当てられたパケットは無効と見なされて廃棄されます。
dst-mac	イーサネット ヘッダーの宛先 MAC アドレスを ARP 本文の宛先 MAC アドレスと比較します。この検証は、ARP 応答に対して実行されます。 イネーブルの場合、異なる MAC アドレスが割り当てられたパケットは無効と見なされて廃棄されます。
ip	ARP 本文を比較して、無効な IP アドレスや予期しない IP アドレスがないかを確認します。0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスがこれに該当します。 送信元 IP アドレスは、すべての ARP 要求と ARP 応答で比較されます。宛先 IP アドレスは ARP 応答でのみ検証されます。
allow-zeros	送信元アドレスが 0.0.0.0 の ARP (ARP プロブ) が拒否されないように IP 検証テストを変更します。

デフォルト

どの検証も実行されません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

これらのキーワードのうちの少なくともいずれか一方を指定する必要があります。各コマンドは直前のコマンドの設定を無効にします。つまり、最初のコマンドで **src-mac** 検証と **dst-mac** 検証がイネーブルになっており、2 番目のコマンドで IP 検証だけがイネーブルになっている場合は、2 番目のコマンドの結果として **src-mac** 検証と **dst-mac** 検証がディセーブルになります。

allow-zeros キーワードは、次のように ARP アクセス コントロール リスト (ACL) と連携しています。

- ARP プローブを拒否するように ARP ACL を設定すると、**allow-zero** キーワードが指定されている場合でも ARP プローブが廃棄されます。
- ARP プローブを明示的に許可するように ARP ACL を設定し、かつ **ip arp inspection validate ip** コマンドを設定した場合は、**allow-zeros** キーワードを入力しないかぎり、ARP プローブが廃棄されます。

このコマンドが **no** 形式の場合は、指定された検証だけがディセーブルになります。これらのオプションがいずれもイネーブルになっていない場合は、すべての検証がディセーブルになります。

例

次の例では、送信元 MAC 検証をイネーブルにする方法を示します。

```
Switch(config)# ip arp inspection validate src-mac
```

設定を確認するには、**show ip arp inspection vlan vlan-range** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show inventory vlan <i>vlan-range</i>	指定された VLAN に対するダイナミック ARP インспекションの設定と動作ステータスを表示します。

ip arp inspection vlan

VLAN 単位でダイナミック アドレス解決プロトコル (ARP) インスペクションをイネーブルにするには、**ip arp inspection vlan** 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場合は、このコマンドの **no** 形式を使用します。

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

シンタックスの説明

<i>vlan-range</i>	VLAN の番号または範囲を指定します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
-------------------	--

デフォルト

すべての VLAN 上で ARP インスペクションがディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ダイナミック ARP インスペクションをイネーブルにする VLAN を指定する必要があります。
ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、EtherChannel ポート、またはプライベート VLAN ポート上でサポートされています。

例

次の例では、VLAN 1 上でダイナミック ARP インスペクションをイネーブルにする方法を示します。

```
Switch(config)# ip arp inspection vlan 1
```

設定を確認するには、**show ip arp inspection vlan** *vlan-range* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP アクセス コントロール リスト (ACL) を定義します。
show inventory vlan <i>vlan-range</i>	指定された VLAN に対するダイナミック ARP インスペクションの設定と動作ステータスを表示します。

ip arp inspection vlan logging

VLAN ごとにロギングするパケットのタイプを制御するには、**ip arp inspection vlan logging** 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。このロギング制御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。

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings
{all | none | permit} | arp-probe}
```

```
no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings | arp-probe}
```

シンタックスの説明

<i>vlan-range</i>	ロギング用に設定する VLAN を指定します。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
acl-match { matchlog none }	アクセス コントロール リスト (ACL) の照合条件に基づいてパケットをロギングするように指定します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • matchlog : アクセス コントロール エントリ (ACE) に指定されたロギング設定に基づいてパケットをロギングします。このコマンドに matchlog キーワードを指定し、permit または deny ARP アクセス リスト コンフィギュレーション コマンドに log キーワードを指定すると、ACL で許可または拒否されたアドレス解決プロトコル (ARP) パケットがロギングされます。 • none : ACL と一致したパケットをロギングしません。
dhcp-bindings { permit all none }	Dynamic Host Configuration Protocol (DHCP) バインディングの照合条件に基づいてパケットをロギングするように指定します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • all : DHCP バインディングと一致したパケットをすべてロギングします。 • none : DHCP バインディングと一致したパケットをロギングしません。 • permit : DHCP バインディングで許可されたパケットをロギングします。
arp-probe	ARP プロブとして明示的に許可されたパケットをロギングするように指定します。

デフォルト

拒否または廃棄されたパケットがすべてロギングされます。ARP プロブ パケットはロギングされません。

コマンドモード

グローバル コンフィギュレーション

■ ip arp inspection vlan logging

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ロギングされるという表現は、エントリがログ バッファに格納されることとシステム メッセージが生成されることを意味しています。

acl-match キーワードと **dhcp-bindings** キーワードは相互に関連しています。つまり、ACL の照合条件を設定しても、DHCP バインディングの設定がディセーブルになりません。ロギング条件をデフォルト値に戻す場合は、このコマンドの **no** 形式を使用します。いずれのオプションも指定しないと、すべてのタイプのロギングがリセットされ、ARP パケットが拒否された日時がロギングされます。オプションを次に示します。

- **acl-match** : ACL の照合条件に基づくロギングがリセットされ、拒否に基づくロギングが実行されます。
- **dhcp-bindings** : DHCP バインディングの照合条件に基づくロギングがリセットされ、拒否に基づくロギングが実行されます。

acl-match キーワードも **dhcp-bindings** キーワードも指定しないと、拒否されたパケットがすべてロギングされます。

ACL の末尾にある暗黙的な **deny** 文には、**log** キーワードが含まれていません。つまり、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドで **static** キーワードを使用すると、ACL によって DHCP バインディングが無効化されます。ARP ACL の末尾に **deny ip any mac any log** ACE を明示的に指定しないかぎり、拒否された一部のパケットがロギングされない場合があります。

例

次の例では、ACL 内の **permit** コマンドと一致したパケットをロギングするように VLAN 1 上の ARP インспекションを設定する方法を示します。

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

設定を確認するには、**show ip arp inspection vlan vlan-range** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP インспекションのログ バッファをクリアします。
ip arp inspection log-buffer	ダイナミック ARP インспекションのログ バッファを設定します。
show inventory log	ダイナミック ARP インспекション ログ バッファの設定と内容を表示します。
show inventory vlan vlan-range	指定された VLAN に対するダイナミック ARP インспекションの設定と動作ステータスを表示します。

ip dhcp snooping

DHCP スヌーピングをグローバルにイネーブルにするには、**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 dhcp snooping

no ip dhcp snooping



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピングは、ディセーブルです。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、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。

ip dhcp snooping vlan *vlan-id* グローバル コンフィギュレーション コマンドを使用して VLAN 上でスヌーピングをイネーブルにするまで DHCP スヌーピングはアクティブになりません。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping vlan	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip igmp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping binding

DHCP スヌーピング バインディング データベースを設定し、バインディング エントリをデータベースに追加するには、**ip dhcp snooping binding** 特権 EXEC コマンドを使用します。バインディング データベースから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 dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id  
expiry seconds
```

```
no ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

mac-address	MAC (メディア アクセス制御) アドレスを指定します。
vlan vlan-id	VLAN 番号を指定します。指定できる範囲は 1 ~ 4094 です。
ip-address	IP アドレスを指定します。
interface interface-id	バインディング エントリを追加または削除するインターフェイスを指定します。
expiry seconds	バインディング エントリが無効になるまでのインターバル (秒) を指定します。指定できる範囲は 1 ~ 4294967295 です。

デフォルト

デフォルトのデータベースは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、スイッチをテストまたはデバッグするときに使用します。

DHCP スヌーピング バインディング データベースでは、各データベース エントリ (別名、バインディング) には、IP アドレス、関連付けられた MAC アドレス、リース時間 (16 進数)、バインディングが適用されるインターフェイス、およびインターフェイスが所属する VLAN が含まれます。データベースには、8192 のバインディングを含めることができます。

設定されたバインディングだけを表示するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを使用します。

例

次の例では、VLAN 1 のポートに、有効期限が 1000 秒の DHCP バインディング設定を生成する方法を示します。

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface  
gigabitethernet0/1 expiry 1000
```

■ ip dhcp snooping binding

設定を確認するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングおよび設定情報を表示します。

ip dhcp snooping database

DHCP スヌーピング バインディング データベース エージェントを設定するには、**ip dhcp snooping database** 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。エージェントのディセーブル化、タイムアウト値のリセット、または書き込み遅延値のリセットを行うには、このコマンドの **no** 形式を使用します。

```
ip dhcp snooping database {{flash:/filename | ftp://user:password@host/filename |
http://[[username:password]@]{hostname | host-ip}[/directory]/image-name.tar |
rcp://user@host/filename | tftp://host/filename} | timeout seconds | write-delay seconds}

no ip dhcp snooping database [timeout | write-delay]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

flash:/filename	データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。
ftp://user:password@host/filename	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
http://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar	データベース エージェントまたはバインディング ファイルが FTP サーバにあることを指定します。
rcp://user@host/filename	データベース エージェントまたはバインディング ファイルが Remote Control Protocol (RCP) サーバにあることを指定します。
tftp://host/filename	データベース エージェントまたはバインディング ファイルが Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバにあることを指定します。
timeout seconds	データベース転送プロセスを打ち切るまでの時間 (秒) を指定します。 デフォルト値は 300 秒です。指定できる範囲は 0 ~ 86400 です。無期限の期間を定義するには、0 を使用します。これは、転送を無期限に続けることを意味します。
write-delay seconds	バインディング データベースが変更されたあとに、転送を遅らせる期間 (秒) を指定します。デフォルト値は 300 秒です。指定できる範囲は 15 ~ 86400 です。

デフォルト

データベース エージェントまたはバインディング ファイルの URL は、定義されていません。

タイムアウト値は、300 秒 (5 分) です。

書き込み遅延値は、300 秒 (5 分) です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング バインディング データベースには、8192 のバインディングを含めることができます。

データベース内のリース時間を正確な時間にするには、Network Time Protocol (NTP; ネットワーク タイム プロトコル) をイネーブルにし、次の機能を設定することを強く推奨します。

- NTP 認証
- NTP ピアおよびサーバ アソシエーション
- NTP ブロードキャスト サービス
- NTP アクセス制限
- NTP パケット送信元 IP アドレス

NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容を書き込みます。

NVRAM とフラッシュ メモリの両方のストレージ容量には限りがあるため、バインディング ファイルを TFTP サーバ上に保存することを推奨します。スイッチがネットワークベースの URL (TFTP や FTP など) の設定済み URL 内のバインディング ファイルにバインディングを書き込む前に、この URL に空のファイルを作成しておく必要があります。

DHCP スヌーピング バインディング データベースを NVRAM に保存するには、**ip dhcp snooping database flash:/filename** コマンドを使用します。**ip dhcp snooping database timeout** コマンドに 0 秒を指定し、データベースを TFTP ファイルに書き込んでいるときに、TFTP サーバがダウンした場合、データベース エージェントは転送を無期限に続けようとしています。この転送が進行中の間、他の転送は開始されません。サーバがダウンしている場合、ファイルを書き込むことができないので、これはあまり重要ではありません。

エージェントをディセーブルにするには、**no ip dhcp snooping database** コマンドを使用します。

タイムアウト値をリセットするには、**no ip dhcp snooping database timeout** コマンドを使用します。

書き込み遅延値をリセットするには、**no ip dhcp snooping database write-delay** コマンドを使用します。

例

次の例では、IP アドレス 10.1.1.1 の *directory* という名前のディレクトリ内にバインディング ファイルを保存する方法を示します。TFTP サーバに *file* という名前のファイルが存在しなければなりません。

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

次の例では、NVRAM に *file01.txt* というバインディング ファイルを保存する方法を示します。

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

設定を確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。

コマンド	説明
<code>ip dhcp snooping binding</code>	DHCP スヌーピング バインディング データベースを設定します。
<code>show ip dhcp snooping database</code>	DHCP スヌーピング データベース エージェントのステータスを表示します。

ip dhcp snooping information option

DHCP オプション 82 データ挿入をイネーブルにするには、**ip dhcp snooping information option** 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。DHCP オプション 82 データ挿入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 information option

no ip dhcp snooping information option



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP オプション 82 データは挿入されます。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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、スイッチがホストからの DHCP 要求を受信すると、オプション 82 情報がパケットに追加されます。オプション 82 情報には、スイッチ MAC (メディア アクセス制御) アドレス (リモート ID サブオプション)、およびパケットが受信された **vlan-mod-port** (回線 ID サブオプション) のポート ID が含まれます。スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

DHCP サーバは、パケットを受信すると、リモート ID または回線 ID (あるいはこの両方) を使用して IP アドレスを割り当て、単一のリモート ID または回線 ID に割り当てることができる IP アドレス数の制限などのポリシーを適用できます。また、DHCP サーバは、DHCP 応答に含まれるオプション 82 フィールドをエコーします。

スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。クライアントとサーバが同一サブネットにある場合、サーバは応答をブロードキャストします。スイッチは、リモート ID または回線 ID フィールドを検査し、オプション 82 データが最初から挿入されていたかを確認します。スイッチは、オプション 82 フィールドを削除し、DHCP 要求を送信した DHCP ホストに接続するスイッチ ポートにパケットを転送します。

例

次の例では、DHCP オプション 82 データ挿入をイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping information option
```


設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping information option allow-untrusted

エッジスイッチに接続されている信頼できないポート上で受信された DHCP パケット (オプション 82 情報が含まれている) を受け入れるようにアグリゲーションスイッチを設定するには、アグリゲーションスイッチ上で **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 dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、エッジスイッチに接続されている信頼できないポートで受信する、オプション 82 情報を持つ DHCP パケットをドロップします。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ホストに接続されたエッジスイッチが、ネットワークのエッジで DHCP オプション 82 情報を挿入するように設定したい場合があります。アグリゲーションスイッチで DHCP スヌーピングなどの DHCP セキュリティ機能をイネーブルにしたい場合もあります。ただし、アグリゲーションスイッチで DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないポートで受信されたオプション 82 情報を持つパケットをドロップし、信頼できるインターフェイスに接続されたデバイスの DHCP スヌーピング バインディングを学習しません。

ホストに接続されたエッジスイッチがオプション 82 情報を挿入する場合に、アグリゲーションスイッチで DHCP スヌーピングを使用するには、アグリゲーションスイッチで **ip dhcp snooping information option allow-untrusted** コマンドを入力します。アグリゲーションスイッチは信頼できないポートで DHCP スヌーピング パケットを受信しますが、ホストのバインディングを学習できます。アグリゲーションスイッチで DHCP セキュリティ機能をイネーブルにすることも可能です。アグリゲーションスイッチが接続されているエッジスイッチ上のポートは、信頼できるポートとして設定する必要があります。



(注)

信頼できないデバイスが接続されたアグリゲーション スイッチに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。

例

次の例では、アクセス スイッチが、エッジ スイッチからの信頼できないパケットのオプション 82 情報を確認せずに、パケットを受け入れるように設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping limit rate

インターフェイスが 1 秒間に受信できる DHCP メッセージの数を設定するには、**ip dhcp snooping limit rate** 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。

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>rate</i>	インターフェイスが 1 秒あたりに受信することのできる DHCP メッセージの数。指定できる範囲は 1 ~ 2048 です。
-------------	--

デフォルト

DHCP スヌーピング レート制限は、ディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

通常、レート制限は信頼できないインターフェイスに適用されます。信頼できるインターフェイスのレート制限を設定する場合、信頼できるインターフェイスはスイッチ内の複数の VLAN 上（一部はスヌーピングされない場合があります）の DHCP トラフィックを集約するので、インターフェイス レート制限を高い値に調整する必要があることに注意してください。

レート制限を超えた場合、インターフェイスが **errdisable** になります。**errdisable recovery dhcp-rate-limit** 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回復をイネーブルにした場合、インターフェイスはすべての原因が時間切れになった際に動作を再試行します。エラー回復メカニズムがイネーブルでない場合、**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までインターフェイスは **errdisable** ステートのままです。

例

次の例は、インターフェイス上でメッセージ レート制限を 1 秒あたり 150 メッセージに設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable recovery	回復メカニズムを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping trust

DHCP スヌーピングを実行するためにポートを信頼できるポートとして設定するには、**ip dhcp snooping 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。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 dhcp snooping trust

no ip dhcp snooping trust



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DHCP スヌーピング信頼は、ディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

DHCP サーバ、その他のスイッチ、またはルータに接続されたポートを信頼できるポートとして設定します。DHCP クライアントに接続されたポートを信頼できないポートとして設定します。

例

次の例では、ポート上に DHCP スヌーピング信頼をイネーブルにする方法を示します。

```
Switch(config-if)# ip dhcp snooping trust
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip dhcp snooping verify

DHCP パケットの送信元 MAC アドレスがクライアントのハードウェア アドレスと一致していることを信頼できないポート上で確認するようにスイッチを設定するには、**ip dhcp snooping verify** 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。スイッチが MAC アドレスを確認しないように設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スイッチは、パケットのクライアント ハードウェア アドレスと一致する信頼されないポートで受信した DHCP パケットの送信元 MAC アドレスを確認します。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

サービスプロバイダー ネットワークで、スイッチが信頼できないポートの DHCP クライアントからパケットを受信した場合、スイッチは自動的に送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致するかを確認します。アドレスが一致する場合、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

例

次の例では、MAC アドレス確認をディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping verify mac-address
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

DHCP スヌーピングを VLAN 上でイネーブルにするには、**ip dhcp snooping vlan** 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 dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>vlan-range</i>	DHCP スヌーピングをイネーブルにする VLAN ID または VLAN 範囲を指定します。指定できる範囲は 1 ~ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。
-------------------	--

デフォルト

すべての VLAN 上で DHCP スヌーピングがディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VLAN 上で DHCP スヌーピングをイネーブルにする前に、まず 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。

例

次の例では、DHCP スヌーピングを VLAN 10 でイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10
```

設定を確認するには、**show ip dhcp snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

ip igmp filter

Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) プロファイル をインターフェイスに適用して、レイヤ 2 インターフェイス上のすべてのホストが 1 つまたは複数の IP マルチキャスト グループに加入できるかどうかを制御するには、**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

シンタックスの説明	<i>profile number</i> 適用する IGMP プロファイル番号。指定できる範囲は 1 ~ 4294967295 です。
-----------	--

デフォルト	IGMP フィルタが適用されていません。
-------	----------------------

コマンド モード	インターフェイス コンフィギュレーション
----------	----------------------

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン	<p>IGMP フィルタはレイヤ 2 の物理インターフェイスのみに適用できます。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 のプロファイルは 1 つまたは複数のポート 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 つのプロファイルのみ適用できます。</p>
------------	---

例	次の例では、IGMP プロファイル 22 をポートに適用する方法を示します。
---	--

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 22
```

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。

関連コマンド

コマンド	説明
ip igmp profile	特定の IGMP プロファイル番号を設定します。
show ip dhcp snooping statistics	指定の IGMP プロファイルの特性を表示します。
show running-config interface interface-id	スイッチのインターフェイス上の実行コンフィギュレーションを（インターフェイスに適用している IGMP プロファイルがある場合はそれを含み）表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

ip igmp max-groups

レイヤ 2 インターフェイスが加入可能なインターネット グループ管理プロトコル (IGMP) グループの最大数を設定したり、転送テーブル内でエントリが最大数に達した場合の IGMP スロットリング動作を設定したりするには、**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 {number | action {deny | replace}}
```

```
no ip igmp max-groups {number | action}
```

シンタックスの説明

number	インターフェイスが参加できる IGMP グループの最大数。指定できる範囲は 0 ~ 4294967294 です。デフォルト設定は無制限です。
action deny	エントリの最大数が IGMP スヌーピング転送テーブルにある場合は、次の IGMP 加入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、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に置き換えます。

デフォルト

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スイッチが学習したあとの、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。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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のみ使用できます。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あとで、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 レポートをスイッチがドロップします。
- 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、スイッチ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 レポートと置き換えます。
- 最大グループ制限がデフォルト (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無効です。

例

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
```

次の例では、転送テーブル内でエントリが最大数に達した場合に IGMP レポートが受信された既存のグループを新規のグループに置換するようにスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(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。

関連コマンド

コマンド	説明
show running-config interface interface-id	インターフェイスが参加できる IGMP グループの最大数やスロットリング アクションなど、スイッチのインターフェイス上で実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。

ip igmp profile

インターネットグループ管理プロトコル (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、**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

シンタックスの説明

profile number 設定する IGMP プロファイル番号。指定できる範囲は 1 ~ 4294967295 です。

デフォルト

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。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

- **deny** : 一致したアドレスを拒否します (デフォルトの条件)。
- **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か、デフォルト設定に戻します。
- **permit** : 一致したアドレスを許可します。
- **range** : プロファイルに対する 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。

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。

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 つのみです。

例

次の例では、IP マルチキャスト アドレスの範囲を指定した IGMP プロファイル 40 の設定方法を示します。

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

■ ip igmp profile

設定を確認するには、**show ip igmp profile** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip igmp filter	指定のインターフェイスに対し、IGMP を適用します。
show ip dhcp snooping statistics	すべての IGMP プロファイルまたは指定の IGMP プロファイル番号の特性を表示します。

ip igmp snooping

インターネットグループ管理プロトコル (IGMP) スヌーピングをスイッチ上で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、**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]
```

シンタックスの説明

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。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。
---------------------	---

デフォルト

スイッチ上で、IGMP スヌーピングはグローバルにイネーブルです。

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。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

```
Switch(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。

```
Switch(config)# ip igmp snooping vlan 1
```

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。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip dhcp snooping statistics	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping last-member-query-interval

インターネットグループ管理プロトコル (IGMP) の設定可能な Leave タイマー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、**ip igmp snooping last-member-query-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*] last-member-query-interval *time*

no ip igmp snooping [vlan *vlan-id*] last-member-query-interval

シンタックスの説明	説明
<i>vlan vlan-id</i>	(任意) 指定された VLAN で IGMP スヌーピングおよび Leave タイマーをイネーブルにします。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。
<i>time</i>	秒単位のタイムアウト間隔。指定できる範囲は 100 ~ 32768 ミリ秒です。

デフォルト デフォルトのタイムアウト設定は 1000 ミリ秒です。

コマンドモード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(46)SE	<i>time</i> の範囲が 100 ~ 32768 秒に変更されました。
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン 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、IGMP スヌーピングはすべての既存 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は、IGMP スヌーピングはすべての既存 VLAN インターフェイスで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。

VLAN 上に Leave タイマーを設定すると、グローバル設定を上書きします。

IGMP の設定可能な Leave タイムは、IGMP バージョン 2 を実行しているデバイス上でのみサポートされています。

設定は、NVRAM に保存されます。

例 次の例では、IGMP Leave タイマーを 2000 ミリ秒でグローバルにイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

次の例では、VLAN 1 上で IGMP Leave タイマーを 3000 ミリ秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

■ ip igmp snooping last-member-query-interval

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。

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan immediate-leave	IGMP 即時脱退処理をイネーブルにします。
ip igmp snooping vlan mrouter	レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをグループのメンバーとして設定します。
show ip igmp snooping	IGMP スヌーピング設定を表示します。

ip igmp snooping querier

レイヤ 2 ネットワークのインターネット グループ管理プロトコル (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 querier [vlan vlan-id] [address ip-address | max-response-time
response-time | query-interval interval-count | tcn query [count count | interval interval]
| timer expiry | version version]
```

```
no ip igmp snooping querier [vlan vlan-id] [address | max-response-time | query-interval
| tcn query { count count | interval interval } | timer expiry | version]
```

シンタックスの説明

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。指定できる範囲は 1 ~ 1001 または 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。指定できる範囲は 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。指定できる範囲は 1 ~ 18000 秒です。
tcn query [count <i>count</i> interval <i>interval</i>]	(任意) Topology Change Notification (TCN; トポロジ変更通知) に関連するパラメータを設定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> count <i>count</i> : TCN の間隔中に実行する TCN クエリーの数を設定します。指定できる範囲は 1 ~ 10 です。 interval <i>interval</i> : TCN クエリーの時間間隔を設定します。指定できる範囲は 1 ~ 255 です。
timer expiry	(任意) IGMP クエリアが期限切れになるまでの時間の長さを設定します。指定できる範囲は 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。

デフォルト

IGMP スヌーピング クエリア機能は、スイッチでグローバルにイネーブルです。

イネーブルになっている場合、マルチキャスト対応デバイスから IGMP トラフィックを検出すると、IGMP スヌーピング クエリアはディセーブルになります。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

クエリアとも呼ばれる IGMP クエリー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せん。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 非準拠デバイスは、**max-response-time** 値としてゼロ以外の値が設定された IGMP 一般クエリーメッセージを拒否する場合があります。デバイスで IGMP 一般クエリー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。

```
Switch(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。

```
Switch(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。

```
Switch(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 クエリー カウントを 25 に設定する方法を示します。

```
Switch(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を 60 秒に設定する方法を示します。

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch(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。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	IGMP スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。

ip igmp snooping report-suppression

インターネット グループ管理プロトコル (IGMP) レポート抑制をイネーブルにするには、**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 ルータへ転送するには、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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IGMP レポート抑制はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

IGMP レポート抑制は、マルチキャスト クエリーに 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、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは IGMP レポート抑制を使用して、マルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル (デフォルト) である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、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 クエリーに 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、スイッチは最初の 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 ルータに送信します。マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチ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 ルータに送信されます。

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。

```
Switch(config)# no ip igmp snooping report-suppression
```

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

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn

インターネットグループ管理プロトコル (IGMP) トポロジ変更通知 (TCN) の動作を設定するには、**ip igmp snooping tcn** 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 tcn {flood query count count | query solicit}
```

```
no ip igmp snooping tcn {flood query count | query solicit}
```

シンタックスの説明

flood query count <i>count</i>	マルチキャストトラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ~ 10 です。
query solicit	TCN イベント中に発生したフラッドモードから回復するプロセスの速度を上げるために、IGMP 脱退メッセージ (グローバル脱退) を送信します。

デフォルト

TCN フラッドクエリー カウントは 2 です。
TCN クエリー要求はディセーブルです。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

TCN イベント後にマルチキャストトラフィックがフラッディングする時間を制御するには、**ip igmp snooping tcn flood query count** 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。**ip igmp snooping tcn flood query count** コマンドを使用して TCN フラッドクエリー カウントを 1 に設定した場合、1 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定すると、TCN イベントによるマルチキャストトラフィックのフラッディングは、7 つの一般的クエリーを受信するまで継続します。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されません。

スパニングツリールートかどうかにかかわらず、グローバル脱退メッセージを送信するようにスイッチをイネーブルにするには、**ip igmp snooping tcn query solicit** 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。また、このコマンドは、TCN イベント中に発生したフラッドモードから回復するプロセスの速度を上げます。

例

次の例では、マルチキャストトラフィックがフラッディングする IGMP の一般的クエリー数を 7 に指定する方法を示します。

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

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 tcn

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn flood	インターフェイスのフラッディングを IGMP スヌーピング スパニングツリー TCN 動作として指定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping tcn flood

マルチキャストフラッドをインターネットグループ管理プロトコル (IGMP) スヌーピング スパニングツリー トポロジ変更通知 (TCN) の動作として設定するには、**ip igmp snooping tcn flood** 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。マルチキャストフラッ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 igmp snooping tcn flood

no ip igmp snooping tcn flood

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

マルチキャストフラッドは、スパニングツリー TCN のイベント中、インターフェイス上でイネーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが TCN を受信すると、2 つの一般的なクエリーが受信されるまで、マルチキャストトラフィックはすべてのポートに対してフラッドします。異なるマルチキャストグループに加入している接続ホストを持つポートがスイッチに多数ある場合、フラッドがリンクの容量を超過し、パケット損失を招くことがあります。

ip igmp snooping tcn flood query count count 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、フラッドクエリーカウントを変更できます。

例

次の例では、インターフェイス上でマルチキャストフラッドをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no ip igmp snooping tcn flood
```

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。

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping tcn	スイッチで IGMP TCM 動作を設定します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。

ip igmp snooping vlan immediate-leave

VLAN 単位でインターネット グループ管理プロトコル (IGMP) スヌーピング即時脱退処理をイネーブルにするには、**ip igmp snooping immediate-leave** 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* immediate-leave

no ip igmp snooping vlan *vlan-id* immediate-leave

シンタックスの説明

<i>vlan-id</i>	(任意) 指定された VLAN で IGMP スヌーピングおよび即時脱退機能をイネーブルにします。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。
----------------	--

デフォルト

IGMP の即時脱退処理はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

VLAN の各ポート上で 1 つのレシーバーの最大値が設定されている場合のみ、即時脱退処理の機能を設定してください。設定は、NVRAM に保存されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

例

次の例では、VLAN 1 で即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

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。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan mrouter

マルチキャスト ルータ ポートを追加したり、マルチキャスト学習方式を設定したりするには、**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。

```
ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp |
pim-dvmrp}}
```

```
no ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp |
pim-dvmrp}}
```

シンタックスの説明

<i>vlan-id</i>	IGMP スヌーピングをイネーブルにして、指定した VLAN のポートをマルチキャスト ルータ ポートとして追加します。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。
interface <i>interface-id</i>	ネクストホップ インターフェイスをマルチキャスト ルータに指定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • fastethernet interface number : ファスト イーサネット IEEE 802.3 インターフェイス • gigabitethernet interface number : ギガビット イーサネット IEEE 802.3z インターフェイス • port-channel interface number : チャネル インターフェイス。指定できる範囲は 0 ~ 6 です。
learn { <i>cgmp</i> <i>pim-dvmrp</i> }	マルチキャスト ルータの学習方式を指定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • cgmp : Cisco Group Management Protocol (CGMP) パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。 • pim-dvmrp : IGMP クエリーおよび Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) パケットでのスヌーピングによりスイッチがマルチキャスト ルータ ポートを学習するように設定します。

デフォルト

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。

デフォルトの学習方式は **pim-dvmrp** です。IGMP クエリーおよび PIM-DVMRP パケットをスヌーピングします。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

CGMP の学習方式は制御トラフィックの削減に役立ちます。

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。

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/22
```

次の例では、マルチキャスト ルータの学習方式を CGMP として指定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
```

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。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip igmp snooping vlan static

インターネット グループ管理プロトコル (IGMP) スヌーピングをイネーブルにし、レイヤ 2 ポートをマルチキャスト グループのメンバーとしてスタティックに追加するには、**ip igmp snooping 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。スタティックなマルチキャスト グループのメンバー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*

シンタックスの説明

<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。指定できる範囲は 1 ~ 1001 または 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 グループのメンバーとして、レイヤ 2 ポートを追加します。
interface <i>interface-id</i>	メンバー ポートのインターフェイスを指定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> fastethernet <i>interface number</i> : ファストイーサネット IEEE 802.3 インターフェイス gigabitethernet <i>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 port-channel <i>interface number</i> : チャネル インターフェイス。指定できる範囲は 0 ~ 6 です。

デフォルト

デフォルトでは、マルチキャスト グループのメンバーとしてスタティックに設定されたポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface gigabitethernet0/1
Configuring port gigabitethernet0/1 on group 0100.5e02.0203
```

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。

関連コマンド

コマンド	説明
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
show ip igmp snooping	スヌーピング設定を表示します。
show ip igmp snooping groups	IGMP スヌーピング マルチキャスト情報を表示します。
show ip igmp snooping mrouter	IGMP スヌーピング ルータ ポートを表示します。
show ip igmp snooping querier	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

ip source binding

スイッチ上でスタティック IP ソース バインディングを設定するには、**ip source binding** 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。スタティック バインディングを削除する場合は、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 source binding mac-address vlan vlan-id ip-address interface interface-id
```

シンタックスの説明

mac-address	MAC (メディア アクセス制御) アドレスを指定します。
vlan vlan-id	VLAN 番号を指定します。指定できる範囲は 1 ~ 4094 です。
ip-address	IP アドレスを指定します。
interface interface-id	IP ソース バインディングを追加または削除するインターフェイスを指定します。

デフォルト

IP ソース バインディングが設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

スタティック IP ソース バインディングのエントリは、IP アドレス、関連付けられた MAC アドレス、および関連付けられた VLAN 番号で構成されています。このエントリは MAC アドレスと VLAN 番号に基づいています。エントリを変更する場合に IP アドレスだけを変更すると、スイッチは新しいエントリを作成せずに、そのエントリを更新します。

例

次の例では、スタティック IP ソース バインディングを追加する方法を示します。

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface gigabitethernet0/1
```

次の例では、スタティック バインディングを追加したあとに、その IP アドレスを変更する方法を示します。

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface gigabitethernet0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface gigabitethernet0/1
```

設定を確認するには、**show ip source binding** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip verify source	インターフェイス上で IP ソース ガードをイネーブルにします。
show ip source binding	スイッチ上の IP ソース バインディングを表示します。
show ip verify source	スイッチまたは特定のインターフェイス上の IP ソース ガード設定を表示します。

ip ssh

Secure Shell (SSH; セキュア シェル) バージョン 1 または SSH バージョン 2 を実行するようにスイッチを設定するには、**ip ssh** 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。このコマンドを使用できるのは、スイッチで暗号化ソフトウェア イメージが実行されている場合だけです。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 ssh version [1 | 2]

no ip ssh version [1 | 2]

シンタックスの説明

- | | |
|---|---|
| 1 | (任意) スイッチが SSH バージョン 1 (SSHv1) を実行するように設定します。 |
| 2 | (任意) スイッチが SSH バージョン 2 (SSHv2) を実行するように設定します。 |

デフォルト

デフォルトのバージョンは、SSH クライアントでサポートされる最新の SSH バージョンです。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力しない場合、またはキーワードを指定しないときは、SSH サーバは SSH クライアントがサポートする最新の SSH バージョンを選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。また、SSHv1 クライアントもサポートします。SSH サーバおよび SSH クライアントの詳細については、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。

SSHv1 サーバによって生成された Rivest、Shamir、Adelman (RSA) キー ペアは、SSHv2 サーバで使用できます。その逆の場合も同様です。

例

次の例では、スイッチが SSH バージョン 2 を実行するように設定する方法を示します。

```
Switch(config)# ip ssh version 2
```

設定を確認するには、**show ip ssh** または **show ssh** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show ip ssh	SSH サーバがイネーブルであるかどうかを表示すると同時に、SSH サーバのバージョンおよび設定情報を表示します。構文情報については、「Cisco IOS Release 12.2 Configuration Guides and Command References」>「Cisco IOS Security Command Reference, Release 12.2」>「Other Security Features」>「Secure Shell Commands」を選択してください。
show ssh	SSH サーバのステータスを表示します。構文情報については、「Cisco IOS Release 12.2 Configuration Guides and Command References」>「Cisco IOS Security Command Reference, Release 12.2」>「Other Security Features」>「Secure Shell Commands」を選択してください。

ip verify source

インターフェイス上で 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。IP ソース ガード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。

ip verify source [port-security]

no ip verify source

シンタックスの説明

port-security	(任意) IP アドレス フィルタリングと MAC アドレス フィルタリングを併用した IP ソース ガードをイネーブルにします。
	port-security キーワードを入力しないと、IP アドレス フィルタリングを使用した IP ソース ガードがイネーブルになります。

デフォルト

IP ソース ガードがディセーブルになっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

送信元 IP アドレス フィルタリングを使用した 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 フィルタリングと送信元 MAC アドレス フィルタリングを併用した IP ソース ガードをイネーブルにするには、**ip verify source port-security** 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 フィルタリングと送信元 MAC アドレス フィルタリングを併用した IP ソース ガードをイネーブルにする場合は、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必要があります。

例

次の例では、送信元 IP アドレス フィルタリングを使用した IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source
```

次の例では、送信元 IP アドレス フィルタリングと送信元 MAC アドレス フィルタリングを併用した IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config-if)# ip verify source port-security
```

設定を確認するには、**show ip source binding** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip source binding	スイッチ上でスタティック バインディングを設定します。
show ip verify source	スイッチまたは特定のインターフェイス上の IP ソース ガード設定を表示します。

ipv6 mld snooping

IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピングをグローバルにイネーブルにするか、または指定された VLAN 上でイネーブルにするには、**ipv6 mld 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。スイッチまたは VLAN 上で MLD スヌーピ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。

ipv6 mld snooping [vlan vlan-id]

no ipv6 mld snooping [vlan vlan-id]



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

vlan vlan-id	(任意) 指定の VLAN で IPv6 MLD スヌーピングをイネーブルまたはディセーブルにします。指定できる VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。
---------------------	---

デフォルト

スイッチ上で、MLD スヌーピングはグローバルにディセーブルです。

すべての VLAN で MLD スヌーピングはイネーブルです。ただし、VLAN スヌーピングが実行される前に、MLD 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。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default}** 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。

MLD スヌーピングがグローバルにディセーブルである場合、すべての既存の VLAN インターフェイスで MLD スヌーピングがディセーブルになります。MLD スヌーピングをグローバルにイネーブルにすると、デフォルトの状態 (イネーブル) であるすべての VLAN インターフェイス上で MLD スヌーピングがイネーブルになります。VLAN 設定は、MLD スヌーピングがディセーブルのインターフェイス上のグローバル コンフィギュレーションを上書きします。

MLD スヌーピングがグローバルにディセーブルである場合、VLAN 上で MLD スヌーピングをイネーブルにできません。MLD スヌーピングがグローバルにイネーブルである場合、個々の VLAN 上で MLD スヌーピングをディセーブルにできます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN (範囲 1006 ~ 4094) が使用されている場合は、Catalyst 6500 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

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。

例

次の例では、MLD 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。

```
Switch(config)# ipv6 mld snooping
```

次の例では、MLD スヌーピングを VLAN でディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 11
```

設定を確認するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
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 snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-count

クライアントがエージングアウトになる前に送信される IP version 6 (IPv6) Multicast Listener Discovery (MLD) Multicast Address Specific Query (MASQ) を設定するには、**ipv6 mld snooping last-listener-query-count** 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。クエリー カウントを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。

ipv6 mld snooping [vlan *vlan-id*] last-listener-query-count *integer_value*

no ipv6 mld snooping [vlan *vlan-id*] last-listener-query-count



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN で last-listener クエリー カウントを設定します。指定できる VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<i>integer_value</i>	指定できる範囲は 1 ~ 7 です。

コマンドのデフォルト

デフォルトのグローバル カウントは 2 です。

デフォルトの VLAN カウントは 0 です (グローバル カウントを使用します)。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default}** 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。

MLD スヌーピングでは、IPv6 マルチキャスト ルータはマルチキャスト グループに所属するホストにクエリーを定期的送信します。ホストがマルチキャスト グループを脱退する場合、ホストは静かに脱退する、または **Multicast Listener Done** メッセージでクエリーに応答できます (IGMP Leave メッセージに相当)。即時脱退が設定されていない場合 (1 つのグループに対し複数のクライアントが同じポート上に存在する場合は設定しない)、設定された last-listener クエリー カウントにより、MLD クライアントが期限切れになる前に送信する MASQ の数が決定します。

last-listener クエリー カウントが VLAN 用に設定されている場合、このカウントはグローバルに設定された値より優先されます。VLAN カウントが設定されていない (デフォルトの 0 に設定されている) 場合は、グローバル カウントが使用されます。

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。

例

次の例では、last-listener クエリー カウントをグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

次の例では、last-listener クエリー カウントを VLAN 10 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

設定を確認するには、**show ipv6 mld snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-interval	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。
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 snooping querier	MLD スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-interval

スイッチまたは VLAN 上で IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピングの last-listener クエリー間隔を設定するには、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドを使用します。この時間間隔は、Multicast Address Specific Query (MASQ) マルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する最大時間です。クエリー時間を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。

ipv6 mld snooping [vlan *vlan-id*] last-listener-query-interval *integer_value*

no ipv6 mld snooping [vlan *vlan-id*] last-listener-query-interval



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN で last-listener クエリー時間を設定します。指定できる VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<i>integer_value</i>	MASQ を送信したあとマルチキャスト グループからポートを削除する前にマルチキャスト ルータが待機する時間 (1000 秒単位) を設定します。指定できる範囲は 100 ~ 32,768 です。デフォルト値は 1000 (1 秒) です。

コマンドのデフォルト

デフォルトのグローバル クエリー間隔 (最大応答時間) は 1000 (1 秒) です。
デフォルトの VLAN クエリー間隔 (最大応答時間) は 0 です (グローバル カウントが使用されます)。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default}** 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。

MLD スヌーピングでは、IPv6 マルチキャスト ルータが MLD Leave メッセージを受信すると、マルチキャスト グループに所属するホストにクエリーを送信します。一定の時間、ポートから MASQ への応答がない場合、ルータはマルチキャスト アドレスのメンバシップ データベースからそのポートを削除します。last listener クエリー間隔は、応答のないポートをマルチキャスト グループから削除する前にルータが待機する最大時間です。

VLAN クエリー間隔が設定されていると、グローバル クエリー間隔より優先されます。VLAN 間隔が 0 に設定されていると、グローバル値が使用されます。

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。

例

次の例では、last-listener クエリー間隔を 2 秒にグローバルに設定する方法を示します。

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

次の例では、VLAN 1 用の last-listener クエリー間隔を 5.5 秒に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

設定を確認するには、**show ipv6 MLD snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
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 snooping querier	IPv6 MLD スヌーピング last-listener クエリー間隔を設定します。

ipv6 mld snooping listener-message-suppression

IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピング リスナー メッセージ抑制をイネーブルにするには、**ipv6 mld snooping listener-message-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。MLD スヌーピング リスナー メッセージ抑制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 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

コマンドのデフォルト

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default}** 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。

MLD スヌーピング リスナー メッセージ抑制は、IGMP レポート抑制に相当します。イネーブルの場合、グループに対する受信 MLDv1 レポートはレポート転送時間ごとに 1 回だけ IPv6 マルチキャスト ルータに転送されます。これにより、重複レポートの転送を避けられます。

例

次の例では、MLD スヌーピング リスナー メッセージ抑制をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

次の例では、MLD スヌーピング リスナー メッセージ抑制をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

設定を確認するには、**show ipv6 mld snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
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 snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping robustness-variable

応答のないリスナーを削除するまでスイッチが送信する IP version 6 (IPv6) Multicast Listener Discovery (MLD) クエリーの数を設定するには、**ipv6 mld snooping robustness-variable** 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。また、VLAN 単位で設定する場合は、VLAN ID を入力します。変数を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。

ipv6 mld snooping [vlan *vlan-id*] robustness-variable *integer_value*

no ipv6 mld snooping [vlan *vlan-id*] robustness-variable



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 指定の VLAN にロバストネス変数を設定します。指定できる VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<i>integer_value</i>	指定できる範囲は 1 ~ 3 です。

コマンドのデフォルト

デフォルトのグローバル ロバストネス変数 (リスナーを削除する前のクエリー数) は、2 です。

デフォルトの VLAN ロバストネス変数 (マルチキャスト アドレスが期限切れになる前のクエリー数) は 0 です。リスナーの期限の判断には、グローバル ロバストネス変数が使用されます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default}** 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。

ロバストネスは、ポートをマルチキャスト グループから削除する前に送信された応答がなかった MLDv1 クエリー数の点から測定されます。設定された回数送信された MLDv1 クエリーに対して受信した MLDv1 レポートがない場合、ポートが削除されます。グローバル値により、スイッチが応答しないリスナーを削除する前に待機するクエリー数が決定し、VLAN 値が設定されていない VLAN すべてに適用します。

VLAN に設定されたロバストネス値はグローバル値より優先されます。VLAN ロバストネス値が 0 (デフォルト) の場合、グローバル値が使用されます。

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。

例 次の例では、スイッチが応答しないリスナー ポートを削除する前に 3 個のクエリーを送信するようグローバル ロバストネス変数を設定する方法を示します。

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

次の例では、VLAN 1 に対してロバストネス変数を設定する方法を示します。この値により、VLAN のグローバル コンフィギュレーションが無効化されます。

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

設定を確認するには、**show ipv6 MLD snooping [vlan vlan-id]** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping last-listener-query-count	IPv6 MLD スヌーピング last-listener クエリー カウントを設定します。
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 snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping tcn

IP version 6 (IPv6) Multicast Listener Discovery (MLD) トポロジ変更通知 (TCN) を設定するには、**ipv6 mld snooping tcn** 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。デフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping tcn {flood query count *integer_value* | query solicit}

no ipv6 mld snooping tcn {flood query count *integer_value* | query solicit}



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

flood query count <i>integer_value</i>	フラッディング クエリー カウントを設定します。これは、クエリーの受信を要求したポートに対しマルチキャスト データを転送する前に送信されるクエリー数です。指定できる範囲は 1 ~ 10 です。
query solicit	TCN クエリーの送信請求をイネーブルにします。

コマンドのデフォルト

TCN クエリー送信請求はディセーブルです。
イネーブルの場合、デフォルトのフラッディング クエリー カウントは 2 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default}** 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。

例

次の例では、TCN クエリー送信請求をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

次の例では、フラッディング クエリー カウントを 5 に設定する方法を示します。

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

設定を確認するには、**show ipv6 MLD snooping [vlan *vlan-id*]** ユーザ EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	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 snooping	MLD スヌーピング設定を表示します。

ipv6 mld snooping vlan

VLAN インターフェイス上で IP version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピングパラメータを設定するには、**ipv6 mld snooping vlan** 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。パラメータを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。

```
ipv6 mld snooping vlan vlan-id [immediate-leave | mrouter interface interface-id | static ipv6-multicast-address interface interface-id]
```

```
no ipv6 mld snooping vlan vlan-id [immediate-leave | mrouter interface interface-id | static ip-address interface interface-id]
```



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

vlan <i>vlan-id</i>	VLAN 番号を指定します。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。
immediate-leave	(任意) VLAN インターフェイス上で MLD の即時脱退処理をイネーブルにします。この機能をインターフェイス上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。
mrouter interface	(任意) マルチキャスト ルータ ポートを設定します。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。
static <i>ipv6-multicast-address</i>	(任意) 指定の IPv6 マルチキャスト アドレスでマルチキャスト グループを設定します。
interface <i>interface-id</i>	レイヤ 2 ポートをグループに追加します。マルチキャスト ルータまたはスタティック インターフェイスは、物理ポートまたはインターフェイス範囲 1 ~ 48 の ポートチャネル インターフェイスになることができます。

コマンドのデフォルト

MLD スヌーピング即時脱退処理はディセーブルです。
デフォルトでは、スタティック IPv6 マルチキャスト グループは設定されていません。
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。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default | vlan}** 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。

VLAN の各ポート上に 1 つのレシーバーだけが存在する場合、即時脱退処理の機能だけを設定してください。設定は、NVRAM に保存されます。

static キーワードは MLD メンバー ポートを静的に設定するために使用されます。

設定およびスタティック ポートとグループは、NVRAM に保存されます。

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ~ 4094）を使用する場合、Catalyst 3750 または Catalyst 3560 スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ~ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

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。

例

次の例では、VLAN 1 で MLD 即時脱退処理をイネーブルにする方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

次の例では、VLAN 1 で MLD 即時脱退処理をディセーブルにする方法を示します。

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

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。

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/01/2
```

次の例では、スタティック マルチキャスト グループを設定する方法を示します。

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/01/2
```

設定を確認するには、**show ipv6 mld snooping vlan *vlan-id*** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ipv6 mld snooping	IPv6 MLD スヌーピングをイネーブルにします。
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
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 snooping	IPv6 MLD スヌーピング設定を表示します。

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、**lacp port-priority** 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。

lacp port-priority priority

no lacp port-priority

シンタックスの説明

priority LACP のポート プライオリティ。指定できる範囲は 1 ~ 65535 です。

デフォルト

デフォルト値は 32768 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

lacp port-priority インターフェイス コンフィギュレーション 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 個のポートをアクティブにして、最大 8 個のポートをスタンバイ モードにすることができます。

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 個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、プライオリティが高い）8 個のポートがチャネル グループにバンドルされ、それよりプライオリティが低いポートはホットスタンバイ モードになります。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します。



(注)

LACP リンクを制御するスイッチ上にポートがある場合のみ、LACP ポート プライオリティは有効です。リンクを制御するスイッチの判別については、**lacp system-priority** 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。

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、**show lacp internal** 特権 EXEC 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。

例

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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lACP port-priority 1000
```

設定を確認するには、**show lACP [channel-group-number] internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
lACP system-priority	LACP システム プライオリティを設定します。
show lACP [channel-group-number] internal	すべてのチャネル グループまたは指定のチャネル グループの内部情報を表示します。

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、**lacp system-priority** 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。

lacp system-priority *priority*

no lacp system-priority

シンタックスの説明

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。

デフォルト

デフォルト値は 32768 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 リンクのスイッチが判別されます。

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 個のポートをアクティブにして、最大 8 個のポートをスタンバイ モードにすることができます。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スイッチは、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。他のスイッチ上のポート プライオリティ（リンクの非制御側終端）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。どちらのスイッチも同じ 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（スイッチの MAC [メディア アクセス制御] アドレス）により制御するスイッチが判別されます。

lacp system-priority コマンドは、スイッチ上のすべての LACP EtherChannel に適用されます。

ホットスタンバイ モードにあるポート（出力表示に H ポート ステート フラグで表されます）を確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

物理ポート上での LACP の設定の詳細については、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 ガイドの「Configuring EtherChannels」の章を参照してください。

例

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。

```
Switch(config)# lacp system-priority 20000
```

設定を確認するには、**show lacp sys-id** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
lacp port-priority	LACP ポート プライオリティを設定します。
show lacp 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。

location (グローバル コンフィギュレーション)

エンドポイントのロケーション情報を設定するには、**location** 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。ロケーション情報を削除する場合は、このコマンドの **no** 形式を使用します。

```
location {admin-tag string | civic-location identifier id | elin-location string identifier id}
```

```
no location {admin-tag string | civic-location identifier id | elin-location string identifier id}
```

シンタックスの説明

admin-tag	管理タグまたはサイト情報を設定します。
civic-location	都市ロケーション情報を設定します。
elin-location	緊急ロケーション情報 (ELIN) を設定します。
identifier id	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ~ 4095 です。
string	サイト情報またはロケーション情報を英数字形式で指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

location civic-location identifier id 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。このモードでは、都市ロケーションおよび郵便ロケーション情報を入力することができます。

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** 情報インターフェイス 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。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 ガイドの「Configuring LLDP and LLDP-MED」の章を参照してください。

例

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。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
```



```
Switch(config-civic)# country US  
Switch(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。

```
Switch (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。

関連コマンド

コマンド	説明
location (インターフェイス コンフィギュレーション)	インターフェイスにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

location (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ロケーション情報を入力するには、**location** インターフェイス コマンドを使用します。インターフェイスの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 {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

no location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

シンタックスの説明

additional-location-information	ロケーションまたは場所に関する追加情報を設定します。
civic-location-id	インターフェイスにグローバル都市ロケーション情報を設定します。
elin-location-id	インターフェイスに緊急ロケーション情報を設定します。
<i>id</i>	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ~ 4095 です。
<i>word</i>	追加のロケーション情報を指定する語またはフレーズを指定します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

location civic-location-id *id* 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、都市ロケーション コンフィギュレーション モードに入ります。このモードでは、追加のロケーション情報を入力することができます。

例

次の例では、インターフェイスに都市ロケーション情報を入力する方法を示します。

```
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

```
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

設定を確認するには、**show location civic interface** 特権 EXEC コマンドを入力します。

次の例では、インターフェイスに緊急ロケーション情報を入力する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

設定を確認するには、**show location elin interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
link state group	エンドポイントにロケーション情報を設定します。
show location	エンドポイントのロケーション情報を表示します。

link state group

リンクステート グループのメンバーとしてポートを設定するには、**link state group** 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。リンクステート グループから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。

link state group [*number*] {**upstream** | **downstream**}

no link state group [*number*] {**upstream** | **downstream**}

シンタックスの説明

number	(任意) リンクステート グループ番号を指定します。グループ番号は、1 ~ 2 です。デフォルトは 1 です。
upstream	ポートを特定のリンクステート グループのアップストリーム ポートとして設定します。
downstream	ポートを特定のリンクステート グループのダウンストリーム ポートとして設定します。

デフォルト

デフォルトのグループは group 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

指定されたリンク ステート グループのアップストリームまたはダウンストリーム インターフェイスとしてポートを設定するには、**link state group** 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。グループ番号が省略されている場合、デフォルトのグループ番号は 1 です。

リンクステート トラッキングをイネーブルにするには、*link-state group* を作成し、リンクステート グループに割り当てるインターフェイスを指定します。ポートの集合 (EtherChannel)、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。リンクステート グループでは、これらのインターフェイスはまとめてバンドルされます。ダウンストリーム インターフェイスは、アップストリーム インターフェイスにバインドされます。サーバに接続されたインターフェイスはダウンストリーム インターフェイスと呼ばれ、ディストリビューションスイッチおよびネットワーク装置に接続されたインターフェイスはアップストリーム インターフェイスと呼ばれます。

ダウンストリーム インターフェイスとアップストリーム インターフェイスの相互運用の詳細については、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 ガイドの「Configuring EtherChannels and Link-State Tracking」の章を参照してください。

設定上の問題を回避するために、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。

- インターフェイスは、複数のリンクステート グループのメンバーにはなれません。
- スイッチごとに設定できるのは、2 個のリンクステート グループのみです。

例

次の例では、group 2 でインターフェイスを **upstream** として設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/11 - 14
Switch(config-if-range)# link state group 2 downstream
Switch(config-if-range)# end
Switch(config-if)# end
```

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。

関連コマンド

コマンド	説明
link state track	リンクステート グループをイネーブルにします。
show link state group	リンクステート グループ情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference for Release 12.2」 > 「Cisco IOS File Management Commands」 > 「Configuration File Commands」を選択してください。

link state track

リンクステート グループをイネーブルにするには、**link state track** ユーザ EXEC コマンドを使用します。リンクステート グルー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。

link state track [*number*]

no link state track [*number*]

シンタックスの説明

number (任意) リンクステート グループ番号を指定します。グループ番号は、1 ~ 2 です。デフォルト値は 1 です。

デフォルト

リンクステート トラッキングは、すべてのグループでディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

リンクステート グループをイネーブルにするには、**link state track** 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。

例

次の例では、リンクステート グループの group 2 をイネーブルにする方法を示します。

```
Switch(config)# link state track 2
```

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。

関連コマンド

コマンド	説明
link state track	リンクステート グループのメンバーとしてインターフェイスを設定します。
show link state group	リンクステート グループ情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference for Release 12.2」 > 「Cisco IOS File Management Commands」 > 「Configuration File Commands」 を選択してください。

logging event

インターフェイス リンク ステータス変更の通知をイネーブルにするには、**logging event** 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。通知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 {bundle-status | link-status | spanning-tree | status | trunk status}

no logging event {bundle-status | link-status | spanning-tree | status | trunk status}

シンタックスの説明

bundle-status	BUNDLE および UNBUNDLE メッセージの通知をイネーブルにします。
link-status	インターフェイス データ リンク ステータス変更の通知をイネーブルにします。
spanning-tree	スパニングツリー イベントの通知をイネーブルにします。
status	スパニングツリー ステート変更メッセージの通知をイネーブルにします。
trunk-status	トランクステータス メッセージの通知をイネーブルにします。

デフォルト

イベント ログギングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、スパニングツリー ログギングをイネーブルにする方法を示します。

```
Switch(config-if)# logging event spanning-tree
```

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、**logging event power-inline-status** 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。PoE 状態イベントのロギングをディセーブルにする場合は、このコマンドの **no** 形式を使用しますが、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。

logging event power-inline-status

no logging event power-inline-status



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

power-inline-status PoE メッセージのロギングをイネーブルにします。

デフォルト

PoE イベントのロギングはイネーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

power-inline-status キーワードは、PoE インターフェイスでのみ使用できます。

例

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。

```
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

関連コマンド

コマンド	説明
power inline	指定した PoE ポートまたはすべての PoE ポートの電力管理モードを設定します。
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。

logging file

ロギング ファイル パラメータを設定するには、**logging 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。

logging file *filesystem:filename* [*max-file-size* | **nomax** [*min-file-size*]] [*severity-level-number* | *type*]

no logging file *filesystem:filename* [*severity-level-number* | *type*]

シンタックスの説明

<i>filesystem:filename</i>	フラッシュ ファイル システムのエイリアスです。ログ メッセージを持つファイルのパスおよび名前を含みます。 ローカル フラッシュ ファイル システムの構文 flash:
<i>max-file-size</i>	(任意) ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ~ 2147483647 です。
nomax	(任意) 最大ファイル サイズ (2147483647) を指定します。
<i>min-file-size</i>	(任意) ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ~ 2147483647 です。
<i>severity-level-number</i>	(任意) ログ ファイルの重大度のレベルを指定します。指定できる範囲は 0 ~ 7 です。各レベルの意味については、 <i>type</i> オプションを参照してください。
<i>type</i>	(任意) ログ タイプを指定します。次のキーワードが有効です。 <ul style="list-style-type: none"> • emergencies : システムは使用不可 (重大度 0) • alerts : 早急な対応が必要 (重大度 1) • critical : 危険な状態 (重大度 2) • errors : エラーが発生している状態 (重大度 3) • warnings : 警告状態 (重大度 4) • notifications : 通常ではあるが、重要なメッセージ (重大度 5) • information : 通知メッセージ (重大度 6) • debugging : デバッグ メッセージ (重大度 7)

デフォルト

ファイル サイズは最小で 2048 バイト、最大で 4096 バイトになります。
デフォルトの重大度のレベルは 7 (**debugging** メッセージ : 数的に低いレベル) です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ログ ファイルはスイッチの内部バッファに ASCII テキスト形式で保存されます。ロギングされたシステム メッセージにアクセスするには、スイッチの CLI (コマンドライン インターフェイス) を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチに障害が生じた場合は、それ以前に **logging file flash:filename** 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ラッシュ メモリにログを保存していないかぎり、ログは失われます。

logging file flash:filename グローバル コンフィギュレーション コマンドで、ログをフラッシュ メモリに保存したあとは、**more flash:filename** 特権 EXEC コマンドを使用してその内容を表示できます。

最小ファイル サイズが、最大ファイル サイズから 1024 引いた数より大きい場合、コマンドはその最小ファイル を拒否し、最大ファイル サイズから 1024 引いたサイズで設定されます。

level を指定すると、そのレベルのメッセージおよび数値的に低いレベルのメッセージが表示されます。

例

次の例では、フラッシュ メモリに情報レベルのログを保存する方法を示します。

```
Switch(config)# logging file flash:logfile informational
```

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。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

mac access-group

MAC アクセス コントロール リスト (ACL) をレイヤ 2 インターフェイスに適用するには、**mac access-group** 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すべてまたは指定の MAC ACL を削除するには、このコマンドの **no** 形式を使用します。MAC ACL を作成するには、**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。

mac access-group {name} in

no mac access-group {name}



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>name</i>	名前付き MAC アクセス リストを指定します。
in	ACL が入力方向に適用されるように指定します。出力 ACL はレイヤ 2 インターフェイスではサポートされていません。

デフォルト

MAC ACL は、インターフェイスには適用されません。

コマンド モード

インターフェイス コンフィギュレーション (レイヤ 2 インターフェイスのみ)

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

MAC ACL は入力レイヤ 2 インターフェイスにだけ適用できます。

レイヤ 2 インターフェイスでは、IP アクセス リストを使用して IP トラフィックをフィルタリングし、MAC アクセス リストを使用して非 IP トラフィックをフィルタリングできます。インターフェイスに IP ACL と MAC ACL の両方を適用すると、同じレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックの両方をフィルタリングできます。同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。

MAC ACL がすでにレイヤ 2 インターフェイスに設定されており、新しい MAC ACL をインターフェイスに適用した場合、以前に設定されていた ACL は新しい ACL で置換されます。

スイッチは、MAC ACL が適用されたインターフェイス上で入力パケットを受信すると、その ACL 内の一致条件を調べます。条件が一致すると、スイッチは ACL に従ってパケットを転送またはドロップします。

指定された ACL が存在しない場合、スイッチはすべてのパケットを転送します。

MAC 拡張 ACL を設定する方法の詳細については、このリリースのソフトウェア コンフィギュレーション ガイドの「Configuring Network Security with ACLs」の章を参照してください。

mac access-group

例

次の例では、*macacl2* と名付けられた MAC 拡張 ACL をインターフェイスに適用する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mac access-group macacl2 in
```

設定を確認するには、**show mac access-group** 特権 EXEC コマンドを入力します。スイッチに設定された ACL を表示するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show access-lists	スイッチで設定される ACL を表示します。
show link state group	スイッチで設定される MAC ACL を表示します。
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

mac access-list extended

非 IP トラフィックの MAC アドレスに基づいてアクセス リストを作成するには、**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。このコマンドを使用すると、拡張 MAC アクセス リスト コンフィギュレーション モードに入ります。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。

mac access-list extended name

no mac access-list extended name



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>name</i>	MAC 拡張アクセス リストに名前を割り当てます。
-------------	---------------------------

デフォルト

デフォルトでは、MAC アクセス リストは作成されません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

名前付き MAC 拡張リストはクラス マップとともに使用されます。

名前付き MAC 拡張 ACL を、レイヤ 2 インターフェイスに適用できます。

mac access-list extended コマンドを入力すると、MAC アクセス リスト 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。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。

- **default** : コマンドのデフォルト値を設定します。
- **deny** : 拒否するパケットを指定します。詳細については、[deny \(MAC アクセス リスト コンフィギュレーション\)](#) MAC アクセス リスト コンフィギュレーション コマンドを参照してください。
- **exit** : MAC アクセス リスト 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か、コマンドのデフォルト値を設定します。
- **permit** : 転送するパケットを指定します。詳細については、[permit \(MAC アクセス リスト コンフィギュレーション\)](#) コマンドを参照してください。

MAC 拡張アクセス リストの詳細については、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。

例

次の例では、名前付き MAC 拡張アクセス リスト *mac1* を作成し、拡張 MAC アクセス リスト コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#
```

次の例では、名前付き MAC 拡張アクセス リスト *mac1* を削除する方法を示します。

```
Switch(config)# no mac access-list extended mac1
```

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。

関連コマンド

コマンド	説明
deny (MAC アクセス リスト コンフィギュレーション)	MAC ACL を設定します (拡張 MAC アクセス リスト コンフィギュレーションモード)。
permit (MAC アクセス リスト コンフィギュレーション)	
show access-lists	スイッチで設定されるアクセス リストを表示します。

mac address-table aging-time

ダイナミック エントリが使用または更新されたあとでそのエントリが MAC アドレス テーブル内で維持される時間を設定するには、**mac address-table aging-time** 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。エージング タイムはすべての VLAN、または指定の VLAN に対して適用されます。

mac address-table aging-time {0 | 10-1000000} [vlan vlan-id]

no mac address-table aging-time {0 | 10-1000000} [vlan vlan-id]

シンタックスの説明	
0	この値はエージングをディセーブルにします。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。
10-1000000	エージング タイム (秒)。指定できる範囲は 10 ~ 1000000 秒です。
vlan vlan-id	(任意) エージング タイムを適用する VLAN ID を指定します。指定できる範囲は 1 ~ 4094 です。

デフォルト デフォルト値は 300 秒です。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン ホストが継続して送信しない場合、エージング タイムを長くして、より長い時間ダイナミック エントリを記録してください。時間を長くすることで、ホストが再送信した場合にフラッシュが起これにくくなります。

特定の VLAN を指定しない場合、このコマンドはすべての VLAN に対してエージング タイムを設定します。

例 次の例では、すべての VLAN にエージング タイムを 200 秒に設定する方法を示します。

```
Switch(config)# mac address-table aging-time 200
```

show mac address-table aging-time 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド	コマンド	説明
	show mac address-table aging-time	すべての VLAN または指定された VLAN の、MAC アドレス テーブルのエージング タイムを表示します。

mac address-table learning vlan

VLAN で MAC (メディア アクセス制御) アドレス学習をイネーブルにするには、**mac address-table learning** 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。これがデフォルトの状態になります。VLAN で MAC アドレス学習をディセーブルにして、MAC アドレスを学習できる VLAN を制御するには、このコマンドの **no** 形式を使用します。

mac address-table learning vlan *vlan-id*

no mac address-table learning vlan *vlan-id*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>vlan-id</i>	1 つの VLAN ID を指定するか、一連の VLAN ID をハイフンまたはカンマで区切って指定します。指定できる VLAN ID は 1 ~ 4094 です。
----------------	--

デフォルト

デフォルトでは、MAC アドレス学習はすべての VLAN でイネーブルです。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

使用上のガイドライン

VLAN で MAC アドレス学習を制御する場合、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。

MAC アドレス学習は、1 つの VLAN ID (例: **no mac address-table learning vlan 223**) または一連の VLAN ID (例: **no mac address-table learning vlan 1-20, 15**) でディセーブルにすることができます。

MAC アドレス学習をディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス学習をディセーブルにすると、ネットワークでフラッディングを引き起こす可能性があります。たとえば、スイッチ仮想インターフェイス (SVI) を設定済みの VLAN で MAC アドレス学習をディセーブルにした場合、スイッチはレイヤ 2 ドメインにすべての IP パケットをフラッディングします。3 つ以上のポートを含む VLAN で MAC アドレス学習をディセーブルにした場合、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。MAC アドレス学習のディセーブル化はポートを 2 つ含む VLAN のみで行い、SVI のある VLAN で MAC アドレス学習をディセーブルにする場合は十分注意してください。

スイッチが内部的に使用する VLAN で MAC アドレス学習はディセーブルにできません。 **no mac address-table learning vlan *vlan-id*** コマンドに入力する VLAN ID が内部 VLAN である場合、スイッチはエラーメッセージを生成してコマンドを拒否します。使用している内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。

プライベート VLAN のプライマリまたはセカンダリ VLAN として設定された VLAN で MAC アドレス学習をディセーブルにする場合、MAC アドレスは、そのプライベート VLAN に属する別の VLAN (プライマリまたはセカンダリ) 上で引き続き学習されます。

RSPAN VLAN で MAC アドレス学習はディセーブルにできません。設定すること自体できません。

セキュア ポートを含む VLAN で MAC アドレス学習をディセーブルにする場合、セキュア ポートで MAC アドレス学習はディセーブルになりません。あとでインターフェイスのポートセキュリティをディセーブルにすると、ディセーブルになった MAC アドレス学習の状態がイネーブルになります。

すべての VLAN、または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning [vlan vlan-id]** コマンドを入力します。

例

次の例では、VLAN 2003 で MAC アドレス学習をディセーブルにする方法を示します。

```
Switch(config)# no mac address-table learning vlan 2003
```

すべての VLAN、または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac-address-table learning [vlan vlan-id]** コマンドを入力します。

関連コマンド

コマンド	説明
show mac address-table learning	すべての VLAN または指定した VLAN の MAC アドレス学習のステータスを表示します。

mac address-table move update

MAC アドレス テーブル移行更新機能をイネーブルにするには、**mac address-table move update** 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。

mac address-table move update {receive | transmit}

no mac address-table move update {receive | transmit}



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

receive	スイッチが MAC アドレステーブル移行更新メッセージを処理するよう指定します。
transmit	プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、スイッチが MAC アドレステーブル移行更新メッセージをネットワークの他のスイッチに送信するよう指定します。

コマンド モード

グローバル コンフィギュレーション

デフォルト

デフォルトでは、MAC アドレステーブル移行更新機能はディセーブルです。

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

MAC アドレステーブル移行更新機能により、プライマリ（フォワーディング）リンクがダウンし、スタンバイ リンクがトラフィックのフォワーディングを開始した場合、スイッチは高速双方向コンバージェンスを提供できます。

プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、アクセス スイッチが MAC アドレステーブル移行更新メッセージを送信するように設定できます。アップリンク スイッチが、MAC アドレステーブル移行更新メッセージを受信および処理するように設定できます。

例

次の例では、アクセス スイッチが MAC アドレステーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次の例では、アップリンク スイッチが MAC アドレステーブル移行更新メッセージを取得および処理する方法を示します。

```
Switch# configure terminal
```

```
Switch(conf)# mac address-table move update receive  
Switch(conf)# end
```

設定を確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear mac address-table move update	MAC アドレステーブル移行更新グローバル カウンタをクリアします。
debug matm move update	MAC アドレステーブル移行更新メッセージ処理をデバッグします。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

mac address-table notification

スイッチ上で MAC アドレス通知機能をイネーブルにするには、**mac address-table notification** 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。

mac address-table notification [*history-size value*] | [*interval value*]

no mac address-table notification [*history-size* | *interval*]

シンタックスの説明

history-size value	(任意) MAC 通知履歴テーブルのエントリの最大数を設定します。指定できる範囲は 0 ~ 500 エントリです。
interval value	(任意) 通知トラップ間隔を設定します。この時間量が過ぎると、スイッチは通知トラップを送信します。指定できる範囲は 0 ~ 2147483647 秒です。

デフォルト

MAC アドレス通知機能はディセーブルです。

トラップ間隔は 1 秒です。

履歴テーブルのエントリ数は 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

MAC アドレス通知機能は、新しい MAC アドレスが転送テーブルに追加されたり、古いアドレスがそこから削除されたりするたびに、SNMP (簡易ネットワーク管理プロトコル) トラップを Network Management System (NMS; ネットワーク管理システム) に送信します。MAC 通知は、ダイナミックまたはセキュア MAC アドレスについてのみ許可されます。自アドレス、マルチキャストアドレス、または他のスタティック アドレスについては、イベントは生成されません。

history-size オプションを設定している場合、既存の MAC アドレス履歴テーブルが削除され、新しいテーブルが作成されます。

mac address-table notification コマンドを使用すれば、MAC アドレス通知機能がイネーブルになります。また、**snmp trap mac-notification** インターフェイス コンフィギュレーション コマンドでインターフェイス上の MAC アドレス通知トラップをイネーブルにし、**snmp-server enable traps mac-notification** グローバル コンフィギュレーション コマンドでスイッチが MAC アドレストラップを NMS に送信するよう設定する必要があります。

例

次の例では、MAC アドレス テーブル通知機能をイネーブルにし、通知トラップの間隔を 60 秒、履歴テーブルのサイズを 100 エントリに設定する方法を示します。

```
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
```

show mac address-table notification 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
show mac address-table notification	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-server enable traps	mac-notification キーワードが追加された場合に SNMP MAC 通知トラップを送信します。
snmp trap mac-notification	特定のインターフェイスの SNMP MAC 通知トラップをイネーブルにします。

mac address-table static

MAC アドレス テーブルにスタティック アドレスを追加するには、**mac address-table 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。スタティック エントリをテーブ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。

mac address-table static mac-addr vlan vlan-id interface interface-id

no mac address-table static mac-addr vlan vlan-id [interface interface-id]

シンタックスの説明

mac-addr	アドレス テーブルに追加する宛先 MAC アドレス (ユニキャストまたはマルチキャスト)。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。
vlan vlan-id	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる範囲は 1 ~ 4094 です。
interface interface-id	受信されたパケットを転送するインターフェイス。有効なインターフェイスは、物理ポートおよびポート チャネルです。

デフォルト

スタティック アドレスは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、MAC アドレス テーブルにスタティック アドレス `c2f3.220a.12f4` を追加する方法を示します。VLAN 4 でこの MAC アドレスを宛先としてパケットを受信すると、パケットは指定されたインターフェイスに転送されます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

設定を確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。

mac address-table static drop

ユニキャスト MAC アドレス フィルタリングをイネーブルにして、特定の送信元 MAC アドレスまたは宛先 MAC アドレスのトラフィックを廃棄するようにスイッチを設定するには、**mac address-table static drop** 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。

mac address-table static mac-addr vlan vlan-id drop

no mac address-table static mac-addr vlan vlan-id

シンタックスの説明

<i>mac-addr</i>	ユニキャスト送信元または宛先 MAC アドレス。この MAC アドレスを持つパケットはドロップされます。
<i>vlan vlan-id</i>	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID は 1 ~ 4094 です。

デフォルト

ユニキャスト MAC アドレス フィルタリングはディセーブルです。スイッチは、特定の送信元または宛先 MAC アドレスのトラフィックをドロップしません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

この機能を使用する場合、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレスはサポートされません。CPU に転送されるパケットもサポートされません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定する場合は、最後に入力されたコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、またはその MAC アドレスを持つパケットをドロップします。2 番めに入力したコマンドは、最初のコマンドを上書きします。

たとえば、**mac address-table static mac-addr vlan vlan-id interface interface-id** グローバル コンフィギュレーション コマンドのあとに **mac address-table static mac-addr vlan vlan-id drop** コマンドを入力した場合は、スイッチは送信元または宛先として指定された MAC アドレスを持つパケットをドロップします。

mac address-table static mac-addr vlan vlan-id drop グローバル コンフィギュレーション コマンドのあとに **mac address-table static mac-addr vlan vlan-id interface interface-id** コマンドを入力した場合は、スイッチがその MAC アドレスをスタティック アドレスとして追加します。

■ mac address-table static drop

例

次の例では、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つパケットをドロップするようにスイッチを設定する方法を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

次の例では、ユニキャスト MAC アドレス フィルタリングをディセーブルにする方法を示します。

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

show mac address-table static 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。

macro apply

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にマクロ設定を適用してこれを追跡するには、**macro apply** 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。

```
macro {apply | trace} macro-name [parameter {value}] [parameter {value}]
      [parameter {value}]
```

シンタックスの説明

apply	指定した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、そのマクロをデバッグするには、 trace キーワードを使用します。
<i>macro-name</i>	マクロ名を指定します。
parameter value	(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。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。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

macro trace macro-name 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実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

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 デフォルト **Smartports** マクロが埋め込まれています。**show parser macro** ユーザ EXEC コマンドを使用すると、マクロおよびマクロに含まれているコマンドを表示できます。

インターフェイスにシスコ デフォルト Smartports 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。

- **show parser macro** ユーザ EXEC コマンドを使用して、スイッチ上のすべてのマクロを表示します。特定のマクロの内容を表示するには、**show parser macro name macro-name** ユーザ EXEC 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ので、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す。

show running-configuration interface interface-id ユーザ EXEC 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。あるインターフェイスでマクロ コマンドが失敗した場合、残りのインターフェイスに適用されていきます。

default interface interface-id 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

macro name 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マクロを作成したあとは、そのマクロを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。

```
Switch(config-if)# macro apply duplex
```

マクロをデバッグするには、**macro trace** 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、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。次の例では、インターフェイス上の **duplex** という名前のユーザ作成マクロをトラブルシューティングする方法を示します。

```
Switch(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。

```
Switch# 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
-----
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25

```

関連コマンド

コマンド	説明
macro description	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追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro auto execute

組み込みマクロのデフォルト値を置換したり、イベント トリガーから組み込みまたはユーザ定義 Auto Smartports マクロへのマッピングを設定したりするには、**macro auto execute** 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。

```
macro auto execute event trigger {[builtin built-in macro name [parameter=value]] |
[[parameter=value] {function contents }]}

```

```
no macro auto execute event trigger {[builtin built-in macro name [parameter=value]] |
[[parameter=value] {function contents }]}

```



(注)

Cisco IOS Release 12.2(50)SE 以降、**macro name** コマンドに代わって **macro auto execute** コマンドが使用されています。コマンドラインには表示されませんが、**macro name** コマンドはまだアクティブになっています。このコマンドは、今後の Cisco IOS ソフトウェア リリースで使用されなくなります。

シンタックスの説明

<i>event trigger</i>	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。 <i>event trigger</i> に次の値を指定します。 <ul style="list-style-type: none"> • CISCO_PHONE_EVENT • CISCO_SWITCH_EVENT • CISCO_ROUTER_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT • WORD : ユーザ定義のイベント トリガーを適用します。
----------------------	---

builtin <i>built-in macro name</i>	(任意) builtin <i>built-in macro name</i> に次の値を指定します。 <ul style="list-style-type: none"> CISCO_PHONE_AUTO_SMARTPORT (任意) パラメータ値 \$ACCESS_VLAN=(1) および \$VOICE_VLAN=(2) を指定します。 CISCO_SWITCH_AUTO_SMARTPORT (任意) パラメータ値 \$NATIVE_VLAN=(1) を指定します。 CISCO_ROUTER_AUTO_SMARTPORT (任意) パラメータ値 \$NATIVE_VLAN=(1) を指定します。 CISCO_AP_AUTO_SMARTPORT (任意) パラメータ値 \$NATIVE_VLAN=(1) を指定します。 CISCO_LWAP_AUTO_SMARTPORT (任意) パラメータ値 \$ACCESS_VLAN=(1) を指定します。 CISCO_DOT1X_DESKTOP_AUTO_SMARTPORT (任意) パラメータ値 \$ACCESS_VLAN=(1) を指定します。 CISCO_DOT1X_EASY_AUTO_SMARTPORT (任意) パラメータ値 \$ACCESS_VLAN=(1) を指定します。 CISCO_DOT1X_MAB_GUEST_AUTO_SMARTPORT (任意) パラメータ値 \$ACCESS_VLAN=(1) を指定します。 CISCO_DOT1X_MAB_TIMEOUT_AUTO_SMARTPORT (任意) パラメータ値 \$ACCESS_VLAN=(1) を指定します。 CISCO_DOT1X_AUTH_FAIL_AUTO_SMARTPORT (任意) パラメータ値 \$ACCESS_VLAN=(1) を指定します。 CISCO_DOT1X_CRITICAL_AUTO_SMARTPORT (任意) パラメータ値 \$CRITICAL_VLAN=(1) を指定します。
<i>parameter=value</i>	(任意) <i>parameter=value</i> : \$ で始まるデフォルト値を置換します。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>])。カッコ内に示された値はデフォルト値です。
<i>{function contents}</i>	(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。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン組み込み Auto Smartports マクロのデフォルト値をスイッチに固有の値で置換するには、**macro auto execute** 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。

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。

shell trigger 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、新規のイベント トリガーを作成できます。組み込みトリガー/マクロの内容とユーザ定義のトリガー/マクロの内容を表示するには、**show shell** 特権 EXEC コマンドを入力します。

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、削除することも変更することもできません。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。
- **Auto Smartports** 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。
- マクロと元の設定との競合が発生すると、一部のマクロ コマンドを適用できない場合や一部のアンチマクロ コマンドを削除できない場合があります。

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 Smartports** マクロを適用した場合は、ポートが EtherChannel のメンバーになりません。
- 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。スイッチで別の VLAN が使用されている場合は、組み込みマクロのデフォルト値を変更する必要があります。組み込みマクロのデフォルト値をすべて表示するには、**show shell functions** 特権 EXEC コマンドを使用します。
- 802.1x 認証または MAB の場合は、他社製のデバイスを検出するための Cisco Attribute-Value (AV; 属性と値) のペア **auto-smart-port=event trigger** をサポートするように RADIUS サーバを設定します。
- CDP、MAB、802.1x 認証をいずれもサポートしていない固定型のデバイス（ネットワーク プリンタなど）の場合は、ポート上で **Auto Smartports** をディセーブルにすることを推奨します。
- 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、該当するスイッチに Cisco スイッチと Cisco IP Phone を接続するための 2 つの組み込み **Auto Smartports** 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。

```
Switch# configure terminal
Switch(config) #!!!the next command modifies the access and voice vlans
Switch(config) #!!!for the built in Cisco IP phone auto smartport macro
Switch(config) # macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config) #
Switch(config) #!!!the next command modifies the Native vlan used for inter switch trunks
Switch(config) # macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Switch(config) #
Switch(config) #!!!the next command enables auto smart ports globally
Switch(config) # macro auto global processing cdp-fallback
Switch(config) #
Switch(config) # exit

Switch# !!!here's the running configuration of the interface connected
```

```
Switch# !!!to another Cisco Switch after the Macro is applied
Switch#
Switch# show running-config interface Gi1/0/1
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、Cisco Digital Media Player (DMP) と呼ばれるユーザ定義のイベント トリガーをユーザ定義のマクロにマッピングする方法を示します。

- a. 802.1x または MAB に対応したスイッチ ポートに DMP を接続します。
- b. RADIUS サーバ上で、属性と値のペアを **auto-smart-port=CISCO_DMP_EVENT** に設定します。
- c. スイッチ上で、イベント トリガー **CISCO_DMP_EVENT** を作成し、次に示すユーザ定義のマクロ コマンドを入力します。
- d. スイッチは、RADIUS サーバからの attribute-value pair=**CISCO_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。

```
Switch(config)# shell trigger CISCO_DMP_EVENT Cisco DMP player
Switch(config)# macro auto execute CISCO_DMP_EVENT {
if [[ $LINKUP -eq 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 -eq NO ]]; then
conf t
 interface $INTERFACE
  no macro description $TRIGGER
  no switchport access vlan 1
  if [[ $AUTH_ENABLED -eq 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
}
```

macro auto execute

```

fi
}
Switch(config)# end

```

表 2-6 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。
-eq	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。
#	# 文字を使用して、コメント テキストを入力します。

表 2-7 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
function	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

関連コマンド

コマンド	説明
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
shell trigger	イベント トリガーを作成します。
show shell	イベント トリガーとマクロに関する情報を表示します。

macro auto global processing

スイッチ上で Auto Smartports マクロをイネーブルにするには、**macro auto global processing** 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。Auto Smartports 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 global processing [cdp-fallback]

no macro auto global processing [cdp-fallback]

シンタックスの説明	cdp-fallback	(任意) ポート認証がイネーブルの状態では RADIUS サーバからイベントトリガーが送信されなかった場合に Cisco Discovery Protocol (CDP) 機能情報を使用します。
------------------	---------------------	---

デフォルト Auto Smartports がディセーブルになっています。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン スイッチ上で Auto Smartports マクロをグローバルにイネーブルにするには、**macro auto global processing** 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。特定のポート上で Auto Smartports マクロをディセーブルにする場合は、**no macro auto processing** コマンドをインターフェイス モードで使用します。

Auto Smartports マクロでは、ポート上で検出されたデバイス タイプに基づいて動的にポートが設定されます。スイッチは、ポート上で新しいデバイスを検出すると、そのポートに適切な Auto Smartports マクロを適用します。ポート上でリンク ダウン イベントが発生した場合、スイッチはそのマクロを削除します。たとえば、ポートに Cisco IP Phone を接続した場合は、Auto Smartports により自動的に IP Phone マクロが適用されます。IP Phone マクロが適用されると、遅延に影響されやすい音声トラフィックを正しく処理できるように QoS (Quality Of Service)、セキュリティ機能、および専用の音声 VLAN がイネーブルになります。

Auto Smartports では、デバイスからマクロへのマッピングにイベントトリガーが使用されます。接続されたデバイスからの Cisco Discovery Protocol (CDP) メッセージに基づくイベントトリガーが最も一般的です。デバイスが検出されると、CDP イベントトリガーが呼び出されます。これは、Cisco IP Phone、Cisco 無線アクセス ポイント、Cisco スイッチ、または Cisco ルータに該当します。それ以外のイベントトリガーでは、MAC 認証バイパス (MAB) および 802.1x 認証メッセージが使用されません。

ポート上で認証がイネーブルになっている場合は、**cdp-fallback** キーワードをイネーブルにしないかぎり、スイッチで CDP メッセージが無視されます。

802.1x または MAB 認証を使用している場合は、Cisco 属性と値 (AV) のペア **auto-smart-port=event trigger** をサポートするように RADIUS サーバを設定します。

■ macro auto global processing

CDP で特定されたデバイスによって複数の機能がアドバタイズされている場合、スイッチはスイッチ、ルータ、アクセス ポイント、Lightweight アクセス ポイント、電話機、ホストのプライオリティ順に機能を選択します。

Auto Smartports マクロがインターフェイスに適用されているかどうかを確認するには、**show running config** ユーザ EXEC コマンドを使用します。

例

次の例では、Auto Smartports をスイッチ上でイネーブルにし、特定のインターフェイス上でディセーブルにする方法を示します。

```
Switch(config)# macro auto global processing
Switch(config)# interface interface_id
Switch(config-if)# no macro auto processing
```

関連コマンド

コマンド	説明
macro auto execute	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設定します。
shell trigger	イベント トリガーを作成します。
show shell	イベント トリガーとマクロに関する情報を表示します。

macro description

インターフェイスに適用されるマクロの説明を入力するには、**macro 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 description *text*

no macro description *text*

シンタックスの説明

description *text* 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。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

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。

```
Switch(config-if)# macro description duplex settings
```

設定を確認するには、**show parser macro description** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global

スイッチにマクロを適用するか、またはスイッチにマクロ設定を適用してこれを追跡するには、**macro global** 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。

```
macro global {apply | trace} macro-name [parameter {value}] [parameter {value}]
[parameter {value}]
```

シンタックスの説明

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。
macro-name	マクロ名を指定します。
parameter value	(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。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

macro trace macro-name 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、スイッチ上で実行されているマクロを適用および表示、あるいは構文または設定エラーを判別するためにマクロをデバッグできます。

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。**show parser macro** ユーザ EXEC コマンドを使用すると、マクロおよびマクロに含まれているコマンドを表示できます。

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。

- **show parser macro** ユーザ EXEC コマンドを使用して、スイッチ上のすべてのマクロを表示します。特定のマクロの内容を表示するには、**show parser macro name macro-name** ユーザ EXEC 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-configuration** ユーザ EXEC 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。

マクロに含まれる各コマンドの **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。

例

macro name 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マクロを作成したあとは、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。

```
Switch# 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

-----
Switch(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** 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、マクロがスイッチ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。次の例では、**ADDRESS** パラメータ値が入力されなかったために **snmp-server host** コマンドが失敗した一方で、残りのマクロがスイッチに適用されていることを示します。

```
Switch(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'
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	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追加します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro global description

スイッチに適用されるマクロの説明を入力するには、**macro global description** 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。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*

シンタックスの説明

description *text* 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。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

次の例では、スイッチに説明を追加する方法を示します。

```
Switch(config)# macro global description udld aggressive mode enabled
```

設定を確認するには、**show parser macro description** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	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追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro name	マクロを作成します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

macro name

設定マクロを作成するには、**macro name** 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。マクロ定義を削除するには、このコマンドの **no** 形式を使用します。

macro name *macro-name*

no macro name *macro-name*



(注)

Cisco IOS Release 12.2(50)SE 以降、**macro name** コマンドに代わって **macro auto execute** コマンドが使用されています。コマンドラインには表示されませんが、**macro name** コマンドはまだアクティブになっています。このコマンドは、今後の Cisco IOS ソフトウェア リリースで使用されなくなります。

シンタックスの説明

<i>macro-name</i>	マクロの名前
-------------------	--------

デフォルト

このコマンドにはデフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(50)SE	このコマンドは廃止されました。

使用上のガイドライン

マクロには、最大 3000 文字を含めることができます。1 行に 1 つのマクロ コマンドを入力します。マクロを終了するには **@** 文字を使用します。マクロ内にコメント テキストを入力するには、行の先頭に **#** 文字を使用します。

ヘルプ文字列を使用してキーワードを指定し、マクロ内で必須キーワードを定義できます。**#macro keywords word** を入力してマクロで使用できるキーワードを定義します。スペースで分離することにより最大で 3 つのヘルプ スtring を入力できます。4 つのキーワードを入力した場合、最初の 3 つのみが表示されます。

マクロ名では、大文字と小文字が区別されます。たとえば、コマンド **macro name Sample-Macro** と **macro name sample-macro** は、2 つの別個のマクロとなります。

マクロを作成する際に、**exit** や **end** コマンド、または **interface interface-id** コマンドを使用してコマンドモードを変更しないでください。これらのコマンドを使用すると、**exit**、**end**、または **interface interface-id** に続くコマンドが異なるコマンドモードで実行されることがあります。

このコマンドの **no** 形式によって、マクロ定義のみが削除されます。マクロがすでに適用されているインターフェイスの設定には、影響はありません。**default interface interface-id** 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。また、元のマクロの対応するコマンドすべての **no** 形式を含む既存のマクロの **anti-macro** を作成できます。次に **anti-macro** をインターフェイスに適用します。

既存のマクロと同じ名前の新しいマクロを作成して、マクロを変更することができます。新規作成されたマクロは既存のマクロを上書きしますが、元のマクロが適用されたインターフェイスの設定には影響を与えません。

例 次の例では、デュプレックス モードおよび速度を定義するマクロを作成する方法を示します。

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

次の例では、**# macro keyword** でマクロを作成する方法を示します。

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

次の例では、インターフェイスにマクロを適用する前に、必須キーワード値を表示する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# macro apply test ?
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID ?
WORD Value of first keyword to replace
```

```
Switch(config-if)# macro apply test $VLANID 2
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
```

```
Switch(config-if)# macro apply test $VLANID 2 $MAX ?
WORD Value of second keyword to replace
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	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追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
show parser macro	すべてのマクロまたは指定したマクロのマクロ定義を表示します。

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、**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。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。

```
match {access-group acl-index-or-name | ip dscp dscp-list | ip precedence ip-precedence-list}
```

```
no match {access-group acl-index-or-name | ip dscp dscp-list | ip precedence ip-precedence-list}
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

access-group <i>acl-index-or-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 (メディア アクセス制御) ACL の番号または名前です。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。
ip dscp <i>dscp-list</i>	着信パケットとのマッチングを行うための、最大 8 つまでの IP Differentiated Service Code Point (DSCP) 値のリストです。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。よく使用する値の場合は、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>	着信パケットとのマッチングを行うための、最大 8 つの IP precedence 値のリストです。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。よく使用する値の場合は、ニーモニック名を入力することもできます。

デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 のマッチングのみがサポートされています。

物理ポート単位でパケット分類を定義するため、クラス マップごとに 1 つずつのみ **match** コマンドがサポートされています。この状況では、**match-all** キーワードと **match-any** キーワードは同じです。

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** コマンドを入力できます。このコマンドは、**match ip dscp 10** コマンドを入力した場合と同じ結果になります。また、**match ip precedence critical** コマンドを入力できます。このコマンドは、**match ip precedence 5** コマ

ンドを入力した場合と同じ結果になります。サポートされているニーモニック名のリストについては、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインヘルプ スtring を参照してください。

例

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。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(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。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(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。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

show class-map 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの比較に使用されるクラス マップを作成します。
show class-map	QoS (Quality of Service) クラス マップを表示します。

mdix auto

インターフェイス上で Automatic Medium-Dependent Interface Crossover (Auto-MDIX) 機能をイネーブルにするには、**mdix auto** 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。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。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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

Auto MDIX は、イネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

自動 MDIX は、すべての 10/100 および 10/100/1000 Mbps インターフェイスでサポートされます。自動 MDIX は、1000BASE-SX または -LX Small Form-factor Pluggable (SFP) モジュールポートではサポートされません。

例

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

インターフェイス上の Auto MDIX の動作ステータスを確認するには、**show controllers ethernet-controller interface-id phy** 特権 EXEC コマンドを入力します。

media-type

デュアルパーパス アップリンク ポートのインターフェイスとタイプを手動で選択したり、最初にリンクが確立されたタイプをスイッチで動的に選択するように設定したりするには、**media-type** 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。

```
media-type {auto-select | rj45 | sfp}
```

```
no media-type
```

シンタックスの説明

auto-select	最初にリンクが確立されたタイプをスイッチで動的に選択します。
rj45	RJ-45 インターフェイスを選択します。
sfp	Small Form-Factor Pluggable (SFP) モジュール インターフェイスを選択します。

デフォルト

デフォルトは **auto-select** による動的選択です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

デュアルパーパス アップリンクを冗長リンクとして使用することはできません。

デュアルパーパス アップリンクの速度とデュプレックスを設定するには、インターフェイス タイプを選択する必要があります。タイプを変更すると、速度とデュプレックスの設定は削除されます。スイッチはいずれのタイプも、速度とデュプレックスの両方の自動ネゴシエーションに基づいて設定します (デフォルト)。

auto-select を選択した場合、スイッチは最初にリンクが確立されたタイプを動的に選択します。リンクの確立が完了すると、スイッチはアクティブ リンクが終了するまでの間、もう一方のタイプをディセーブルにします。アクティブ リンクが終了すると、スイッチはいずれかのリンクが確立されるまでの間、両方のタイプをイネーブルにします。**auto-select** モードでは、スイッチはいずれのタイプも速度とデュプレックスの自動ネゴシエーションに基づいて設定します (デフォルト)。

rj45 を選択した場合、スイッチは SFP モジュール インターフェイスをディセーブルにします。このポートにケーブルを接続しても、RJ-45 側がダウンしている場合または接続されていない場合であっても、リンクを確立することはできません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様に動作します。このインターフェイス タイプに合った速度とデュプレックスが設定できます。

sfp を選択した場合、スイッチは RJ-45 インターフェイスをディセーブルにします。このポートにケーブルを接続しても、SFP モジュール側がダウンしている場合または SFP モジュールが存在しない場合であっても、リンクを確立することはできません。搭載された SFP モジュール タイプに応じて、このインターフェイス タイプに合った速度とデュプレックスが設定できます。

スイッチの電源投入時、または **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 コマンドでデュアルパーパス アップリンク ポートをイネーブルにした場合は、SFP モジュール インターフェイスを優先します。その他の場合は、最初にリンクが確立されたタイプを動的に選択します。

auto-select を設定した場合、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドは設定できません。

このスイッチと 100BASE-X (-X は -BX、-FX、-FE、-LX のいずれか) SFP モジュールを組み合わせると、次のように動作します。

- 100BASE -X SFP がモジュール スロットに挿入され、RJ-45 側にリンクが存在しない場合には、スイッチは RJ-45 インターフェイスをディセーブルにし、SFP モジュール インターフェイスを選択します。SFP 側にケーブルが接続されておらず、リンクがない場合でも、このような動作になります。
- 100BASE-X SFP モジュールが挿入されており、RJ-45 側にリンクが存在する場合には、スイッチはそのリンクを使用します。リンクがダウンすると、スイッチは RJ-45 側をディセーブルにし、SFP モジュール インターフェイスを選択します。
- 100BASE-X SFP モジュールが取り外されると、スイッチはタイプの動的選択 (**auto-select**) に戻り、RJ-45 側を再度イネーブルにします。

スイッチは 100BASE-FX-GE SFP モジュールに対しては、このような動作はしません。

例

次の例では、SFP インターフェイスを選択するよう設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# media-type sfp
```

設定を確認するには、**show interfaces interface-id capabilities** または **show interfaces interface-id transceiver properties** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces capabilities	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の機能を表示します。
show interfaces transceiver properties	インターフェイスの速度とデュプレックスの設定およびメディアタイプを表示します。

mls qos

スイッチ全体で QoS (Quality Of Service) をイネーブルにするには、**mls qos** 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。**mls qos** コマンドを入力すると、システム内のすべてのポートでデフォルト パラメータが使用されて QoS がイネーブルになります。スイッチ全体のすべての QoS 関連の統計をリセットし、QoS 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。

mls qos

no mls qos

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

QoS はディセーブルです。パケットが変更されない (パケット内の CoS、DSCP、および IP precedence 値は変更されない) ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックは **Pass-Through** モードでスイッチングされます (パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます)。

mls qos グローバル コンフィギュレーション コマンドによって QoS がイネーブル化され、その他のすべての QoS 設定値がデフォルト値に設定されている場合、トラフィックはポリシングされず、ベスト エフォート (DSCP 値と CoS 値は 0 に設定される) として分類されます。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし (**untrusted**) の状態です。デフォルトの入力キューおよび出力キューの設定値が有効となります。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

QoS 分類、ポリシング、マークダウンまたはドロップ、キューイング、トラフィック シェーピング機能を使用するには、QoS をグローバルにイネーブルにする必要があります。**mls qos** コマンドを入力する前に、ポリシー マップを作成しそれをポートに適用できます。ただし、**mls qos** コマンドを入力していない場合、QoS 処理はディセーブルになります。

no mls qos コマンドを入力しても、QoS を設定するために使用したポリシー マップとクラス マップは設定から削除されません。ただし、システム リソースを節約するため、ポリシー マップに対応するエントリはスイッチ ハードウェアから削除されます。以前の設定で QoS を再度イネーブルにする場合、**mls qos** コマンドを使用します。

このコマンドでスイッチの QoS 状態を切り替えることで、キューのサイズが修正 (再割り当て) されます。キュー サイズの変更時には、ハードウェアを再設定する期間中キューは一時的にシャットダウンされ、スイッチはこのキューに新たに到着したパケットをドロップします。

例

次の例では、スイッチ上で QoS をイネーブルにする方法を示します。

```
Switch(config)# mls qos
```

■ mls qos

設定を確認するには、**show mls qos** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mls qos	QoS 情報を表示します。

mls qos aggregate-policer

ポリサー パラメータを定義するには、**mls qos aggregate-policer** 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。これは、同一のポリシー マップ内の複数のクラスで共有できます。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action {drop | policed-dscp-transmit}

no mls qos aggregate-policer aggregate-policer-name

シンタックスの説明	
<i>aggregate-policer-name</i>	police aggregate ポリシーマップ クラス コンフィギュレーション コマンドが参照する集約ポリサーの名前です。
<i>rate-bps</i>	平均トラフィック伝送速度をビット/秒 (b/s) で指定します。指定できる範囲は 1000000 ~ 1000000000 です。
<i>burst-byte</i>	通常のバーストサイズ (バイト) を指定します。指定できる範囲は 8000 ~ 1000000 です。
exceed-action drop	指定された伝送速度を超えると、スイッチがパケットをドロップするよう指定します。
exceed-action policed-dscp-transmit	指定された伝送速度を超えると、スイッチがパケットの Differentiated Service Code Point (DSCP) を、ポリシング設定 DSCP マップに指定された値に変更して、パケットを送信するよう指定します。

デフォルト 集約ポリサーは定義されません。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン ポリサーが複数のクラスによって共有されている場合は、集約ポリサーを定義します。あるポートのポリサーを別のポートの他のポリサーと共有することはできません。2 つの異なるポートからのトラフィックは、ポリシング目的では集約できません。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー (255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー) をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません (ポートがいずれかのポリサーに割り当てられるとは保証されていません)。

集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

ポリシー マップ内で使用中の場合、集約ポリサーは削除できません。最初に、**no police aggregate aggregate-policer-name** ポリシーマップ クラス コンフィギュレーション コマンドを使用してすべてのポリシー マップから集約ポリサーを削除してから、**no mls qos aggregate-policer aggregate-policer-name** コマンドを使用する必要があります。

ポリシングはトークンバケット アルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** 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。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** 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。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。

例

次の例では、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
police aggregate	異なるクラスによって共有されるポリサーを作成します。
show mls qos aggregate-policer	QoS (Quality of Service) 集約ポリサー設定を表示します。

mls qos cos

ポートのデフォルト サービス クラス (CoS) 値を定義したり、ポート上のすべての着信パケットにデフォルト CoS 値を割り当てたりするには、**mls qos cos** 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。

```
mls qos cos {default-cos | override}
```

```
no mls qos cos {default-cos | override}
```

シンタックスの説明

<i>default-cos</i>	デフォルト CoS 値をポートに割り当てます。パケットがタグ付けされていない場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ~ 7 です。
override	着信パケットの CoS を無効にし、すべての着信パケットにデフォルトのポート CoS 値を適用します。

デフォルト

ポート CoS 値は 0 です。
CoS 無効化はディセーブルに設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

デフォルト値を使用して、タグなし（着信パケットが CoS 値を持たない場合）で着信したすべてのパケットに CoS 値と Differentiated Service Code Point (DSCP) 値を割り当てることができます。また、**override** キーワードを使用すると、デフォルトの CoS 値と DSCP 値をすべての着信パケットに割り当てることができます。

特定のポートに届くすべての着信パケットに、他のポートからのパケットより高いプライオリティを与える場合には、**override** キーワードを使用します。たとえポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されていても、このコマンドは以前に設定済みの信頼状態を無効にし、すべての着信 CoS 値に **mls qos cos** コマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、パケットの CoS 値は、出力ポートで、ポートのデフォルト CoS を使用して変更されます。

例

次の例では、ポートのデフォルト ポート CoS 値を 4 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

次の例では、ポートに到着するすべてのパケットにポートのデフォルト CoS 値 4 を割り当てる方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

設定を確認するには、**show mls qos interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mls qos interface	QoS (Quality of Service) 情報を表示します。

mls qos dscp-mutation

Differentiated Services Code Point (DSCP) の信頼できるポートに DSCP/DSCP 変換マップを適用するには、**mls qos dscp-mutation** 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。マップをデフォルト設定 (DSCP 変換なし) に戻すには、このコマンドの **no** 形式を使用します。

mls qos dscp-mutation *dscp-mutation-name*

no mls qos dscp-mutation *dscp-mutation-name*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>dscp-mutation-name</i>	DSCP/DSCP 変換マップの名前。このマップは、以前は mls qos map dscp-mutation 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ていました。
---------------------------	--

デフォルト

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

2 つの QoS (Quality of Service) ドメインが異なる DSCP 定義を持つ場合は、DSCP/DSCP 変換マップを使用して、一方の DSCP 値のセットをもう一方のドメインの定義に適合するように変換します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します (入力変換)。

入力変換では、新しい DSCP 値がパケット内の値を上書きし、QoS はこの新しい値を持つパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

入力ポートには複数の DSCP/DSCP 変換マップを設定できます。

マップは、DSCP の信頼性のあるポートにのみ適用します。DSCP 変換マップを信頼できないポート、サービス クラス (CoS) または IP precedence の信頼できるポートに適用すると、コマンドはすぐには影響せず、そのポートが DSCP の信頼できるポートになってから効果を発揮します。

例

次の例では、DSCP/DSCP 変換マップ *dscpmutation1* を定義し、そのマップをポートに適用する方法を示します。

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

次の例では、DSCP/DSCP 変換マップ *dscpmutation1* をポートから削除し、そのマップをデフォルトに戻す方法を示します。

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos map dscp-mutation	DSCP/DSCP 変換マップを定義します。
mls qos trust	ポートの信頼状態を設定します。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos map

サービス クラス (CoS) /Differentiated Services Code Point (DSCP) マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシングされた DSCP マップを定義するには、**mls qos map** グローバル コンフィギュレーション コマンドを使用します。デフォルトのマップに戻すには、このコマンドの **no** 形式を使用します。

```
mls qos map {cos-dscp dscp1...dscp8 | dscp-cos dscp-list to cos | dscp-mutation
dscp-mutation-name in-dscp to out-dscp | ip-prec-dscp dscp1...dscp8 | policed-dscp
dscp-list to mark-down-dscp}
```

```
no mls qos map {cos-dscp | dscp-cos | dscp-mutation dscp-mutation-name | ip-prec-dscp |
policed-dscp}
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

cos-dscp <i>dscp1...dscp8</i>	CoS/DSCP マップを定義します。 <i>dscp1...dscp8</i> には、CoS 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。
dscp-cos <i>dscp-list to cos</i>	DSCP/CoS マップを定義します。 <i>dscp-list</i> には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。さらに、 to キーワードを入力します。 <i>cos</i> には、DSCP 値と対応する 1 つの CoS 値を入力します。指定できる範囲は 0 ~ 7 です。
dscp-mutation <i>dscp-mutation-name in-dscp to out-dscp</i>	DSCP/DSCP 変換マップを定義します。 <i>dscp-mutation-name</i> には、変換マップ名を入力します。 <i>in-dscp</i> には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、 to キーワードを入力します。 <i>out-dscp</i> には、1 つの DSCP 値を入力します。 指定できる範囲は 0 ~ 63 です。
ip-prec-dscp <i>dscp1...dscp8</i>	IP precedence/DSCP マップを定義します。 <i>dscp1...dscp8</i> には、IP precedence 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。
policed-dscp <i>dscp-list to mark-down-dscp</i>	ポリシング設定 DSCP マップを定義します。 <i>dscp-list</i> には、各値をスペースで区切って最大 8 つの DSCP 値を入力します。さらに、 to キーワードを入力します。 <i>mark-down-dscp</i> には、対応するポリシング設定 (マークダウンされた) DSCP 値を入力します。 指定できる範囲は 0 ~ 63 です。

デフォルト

表 2-8 に、デフォルトの CoS/DSCP マップを示します。

表 2-8 デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

表 2-9 に、デフォルトの DSCP/CoS マップを示します。

表 2-9 デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 ~ 7	0
8 ~ 15	1
16 ~ 23	2
24 ~ 31	3
32 ~ 39	4
40 ~ 47	5
48 ~ 55	6
56 ~ 63	7

表 2-10 に、デフォルトの IP precedence/DSCP マップを示します。

表 2-10 デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

コマンドモード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン マップはすべてグローバルに定義されています。DSCP/DSCP 変換マップを除くすべてのマップは、すべてのポートに適用されます。DSCP/DSCP 変換マップは、特定のポートに適用されます。

例 次の例では、IP precedence/DSCP マップを定義し、IP precedence 値 0～7 を DSCP 値 0、10、20、30、40、50、55、および 60 にマッピングする方法を示します。

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

次の例では、ポリシング設定 DSCP マップを定義する方法を示します。DSCP 値 1、2、3、4、5、および 6 は DSCP 値 0 にマークダウンされます。明示的に設定されていないマーク付きの DSCP 値は変更されません。

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

次の例では、DSCP/CoS マップを定義する方法を示します。DSCP 値 20、21、22、23、および 24 は CoS 1 にマッピングされます。DSCP 値 10、11、12、13、14、15、16、および 17 は CoS 0 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

次の例では、CoS/DSCP マップを定義する方法を示します。CoS 値 0～7 は、DSCP 値 0、5、10、15、20、25、30、および 35 にマッピングされます。

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないエントリはすべて変更されません（ヌル マップ内の指定のままです）。

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos dscp-mutation	DSCP/DSCP 変換マップを DSCP の信頼性のあるポートに適用します。
show mls qos maps	QoS (Quality of Service) マッピング情報を表示します。

mls qos queue-set output buffers

キューセット（各ポートの4つの出力キュー）にバッファを割り当てるには、**mls qos queue-set output buffers** 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。

```
mls qos queue-set output qset-id buffers allocation1 ... allocation4
```

```
no mls qos queue-set output qset-id buffers
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>qset-id</i>	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー4つの特性すべてを定義します。指定できる範囲は1～2です。
<i>allocation1</i> ... <i>allocation4</i>	各キュー（キュー1～4の4つのキュー）のバッファスペース割り当て（%）です。 <i>allocation1</i> 、 <i>allocation3</i> 、および <i>allocation4</i> の場合、指定できる範囲は0～99です。 <i>allocation2</i> の場合、指定できる範囲は1～100です（CPU バッファを含む）。各値はスペースで区切ります。

デフォルト

すべての割り当て値は、4つのキューに均等にマッピングされます（25、25、25、25）。各キューがバッファスペースの1/4を持ちます。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

4つの割り当て値を指定します。各値はスペースで区切ります。

トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。

異なる特性を持つ異なるクラスのトラフィックを設定するには、**mls qos queue-set output *qset-id* threshold** グローバル コンフィギュレーション コマンドとともに、このコマンドを使用します。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

■ mls qos queue-set output buffers

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。バッファ スペースを出力キュー 1 に 40% 割り当て、出力キュー 2、3、および 4 にそれぞれ 20% ずつ割り当てます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface buffers	QoS (Quality of Service) 情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos queue-set output threshold

Weighted Tail-drop (WTD; 重み付きテール ドロップ) しきい値の設定、バッファの可用性の保証、およびキューセット (各ポートの4つの出力キュー) への最大メモリ割り当ての設定を行うには、**mls qos queue-set output threshold** 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。

```
mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2
reserved-threshold maximum-threshold
```

```
no mls qos queue-set output qset-id threshold [queue-id]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>qset-id</i>	キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー4つの特性すべてを定義します。指定できる範囲は1～2です。
<i>queue-id</i>	コマンドが実行されるキューセット内の特定のキューです。指定できる範囲は1～4です。
<i>drop-threshold1</i> <i>drop-threshold2</i>	キューに割り当てられたメモリの割合 (%) で表される2つの WTD しきい値です。指定できる範囲は1～3200%です。
<i>reserved-threshold</i>	キューに対して保証 (予約) されるメモリ量です。割り当てられたメモリの割合 (%) で表されます。指定できる範囲は1～100%です。
<i>maximum-threshold</i>	フル状態のキューが、予約量を超えるバッファを取得できるようにします。これは、キューがパケットをドロップせずに保持できる最大メモリです。指定できる範囲は1～3200%です。

デフォルト

QoS (Quality of Service) がイネーブルなときは、WTD もイネーブルです。

表 2-11 は、デフォルトの WTD しきい値の設定値を示しています。

表 2-11 デフォルトの出力キュー WTD しきい値設定値

機能	キュー 1	キュー 2	キュー 3	キュー 4
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	100%	50%	50%
最大しきい値	400%	400%	400%	400%

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

mls qos queue-set output *qset-id* buffers グローバル コンフィギュレーション コマンドは、キューセット内の 4 つのキューに固定量のバッファを割り当てます。

ドロップしきい値 (%) は 100% を超過することができ、最大値まで指定することができます (最大しきい値が 100% を超える場合)。

バッファ範囲により、キューセット内の個々のキューが共通のプールをさらに利用できる場合でも、各キューの最大パケット数は内部で 400%、つまりバッファに割り当てられた数の 4 倍に制限されます。1 つのパケットは 1 つまたは複数のバッファを使用できます。

Cisco IOS Release 12.2(25)SEE1 以降で、*drop-threshold*、*drop-threshold2*、*maximum-threshold* パラメータの範囲が増加しました。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

スイッチは、バッファ割り当て方式を使用して、出力キューごとに最小バッファ量を予約し、いずれかのキューまたはポートがすべてのバッファを消費しその他のキューがバッファを使用できなくなるのを防ぎ、バッファ スペースを要求元のキューに許可するかどうかを決定します。スイッチは、ターゲットキューが予約量を超えるバッファを消費していないかどうか (アンダーリミット)、その最大バッファをすべて消費したかどうか (オーバーリミット)、共通のプールが空 (空きバッファがない) か空でない (空きバッファ) かを判断します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール (空でない場合) からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。キュー 2 のドロップしきい値を割り当てられたメモリの 40% と 60% に設定し、割り当てられたメモリの 100% を保証 (予約) して、このキューがパケットをドロップせずに保持可能な最大メモリを 200% に設定します。

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos rewrite ip dscp

着信 IP パケットの Differentiated Services Code Point (DSCP) フィールドを変更する（書き換える）ようにスイッチを設定するには、**mls qos rewrite ip dscp** 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。スイッチがパケットの DSCP フィールドを変更（書き換え）しないように設定し、DSCP 透過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。

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

DSCP 透過がディセーブルになっています。スイッチは着信 IP パケットの DSCP フィールドを変更します。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

DSCP 透過は、出力でのパケットの DSCP フィールドにのみ影響を与えます。**no mls qos rewrite ip dscp** コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて QoS (Quality of Service) に基づきます。

DSCP 透過の設定に関係なく、スイッチは、トラフィックのプライオリティを表すサービス クラス (CoS) 値の生成に使用するパケットの内部 DSCP 値を変更します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

たとえば、QoS がイネーブルになっており、着信パケットの DSCP 値が 32 の場合、スイッチはポリシー マップ設定に基づいて内部 DSCP 値を 16 に変更します。DSCP 透過がイネーブルになっている場合、送信 DSCP 値は 32（着信 DSCP 値と同じ）です。DSCP 透過がディセーブルになっている場合、内部 DSCP 値に基づいて、送信 DSCP 値は 16 になります。

例

次の例では、DSCP 透過性をイネーブルにして、スイッチで着信 IP パケットの DSCP 値を変更しないように設定する方法を示しています。

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
```

次の例では、DSCP 透過性をディセーブルにして、スイッチで着信 IP パケットの DSCP 値を変更するように設定する方法を示しています。

```
Switch(config)# mls qos
Switch(config)# mls qos rewrite ip dscp
```

設定を確認するには、**show running config | include rewrite** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos	QoS をグローバルにイネーブルにします。
show mls qos	QoS 情報を表示します。
show running-config include rewrite	DSCP 透過性設定を表示します。構文情報については、「Cisco IOS Release 12.2 Configuration Guides and Command References」>「Cisco IOS Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

mls qos srr-queue input bandwidth

入力キューに Shaped Round Robin (SRR; シェイプド ラウンド ロビン) ウェイトを割り当てるには、**mls qos srr-queue input bandwidth** 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。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。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。

mls qos srr-queue input bandwidth weight1 weight2

no mls qos srr-queue input bandwidth



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

weight1 weight2 *weight1* および *weight2* の比率によって、SRR スケジューラがパケットを入力キュー 1 および入力キュー 2 から送り出す頻度の比率が決まります。指定できる範囲は 1 ~ 100 です。各値はスペースで区切ります。

デフォルト

weight1 と *weight2* は 4 です (帯域幅の 1/2 ずつ 2 つのキューに均等に分配されます)。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

SRR は、**mls qos srr-queue input priority-queue queue-id bandwidth weight** グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定された重みに従ってプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth weight1 weight2** グローバル コンフィギュレーション コマンドで設定されたウェイトで指定しているサービスを行います。

どの入力キューがプライオリティ キューであるかを指定するには、**mls qos srr-queue input priority-queue** 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。

例

次の例では、キューの入力帯域幅を割り当てる方法を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/ (25+75)、キュー 2 が 75/ (25+75) です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

次の例では、キュー 2 はキュー 1 の 3 倍の帯域幅を持っています。キュー 2 には、キュー 1 の 3 倍の頻度でサービスが提供されます。

■ mls qos srr-queue input bandwidth

次の例では、キューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/(4+4) です。SRR は最初、設定された 10% の帯域幅をキュー 1 (プライオリティ キュー) にサービスします。その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface [interface-id] queueing** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input cos-map	サービス クラス (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	Weighted Tail-Drop (WTD) しきい値のパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	QoS (Quality of Service) 情報を表示します。

mls qos srr-queue input buffers

入力キュー間にバッファを割り当てるには、**mls qos srr-queue input buffers** 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。

mls qos srr-queue input buffers *percentage1 percentage2*

no mls qos srr-queue input buffers



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>percentage1</i>	入力キュー 1 および入力キュー 2 に割り当てられるバッファの割合 (%)
<i>percentage2</i>	です。指定できる範囲は 0 ~ 100 です。各値はスペースで区切ります。

デフォルト

バッファの 90% がキュー 1 に、バッファの 10% がキュー 2 に割り当てられます。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。

例

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

設定を確認するには、**show mls qos interface [*interface-id*] buffers** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR) ウェイトを割り当てます。
mls qos srr-queue input cos-map	サービス クラス (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。

コマンド	説明
<code>mls qos srr-queue input dscp-map</code>	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
<code>mls qos srr-queue input priority-queue</code>	入力プライオリティ キューを設定し、帯域幅を保証します。
<code>mls qos srr-queue input threshold</code>	Weighted Tail-Drop (WTD) しきい値のパーセントを入力キューに割り当てます。
<code>show mls qos input-queue</code>	入力キューの設定を表示します。
<code>show mls qos interface buffers</code>	QoS (Quality of Service) 情報を表示します。

mls qos srr-queue input cos-map

サービス クラス (CoS) 値を入力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングするには、**mls qos srr-queue input cos-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。

```
mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue input cos-map
```

シンタックスの説明

queue <i>queue-id</i>	キュー番号を指定します。 <i>queue-id</i> で指定できる範囲は 1 ~ 2 です。
<i>cos1...cos8</i>	CoS 値を入力キューへマッピングします。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。
threshold <i>threshold-id</i> <i>cos1...cos8</i>	CoS 値をキューのしきい値 ID にマッピングします。 <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。

デフォルト

表 2-12 では、デフォルトの CoS 入力キューのしきい値のマッピングを示します。

表 2-12 デフォルトの CoS 入力キューのしきい値

CoS 値	キュー ID - しきい値 ID
0 ~ 4	1-1
5	2-1
6、7	1-1

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

入力ポートに割り当てられた CoS によって、入力または出力のキューおよびしきい値が選択されます。しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。**mls qos srr-queue input threshold** 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、入力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当てることができます。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、CoS 値 0 ~ 3 を、入力キュー 1 とドロップしきい値 50% のしきい値 ID 1 にマッピングする方法を示します。CoS 値 4 と 5 は、入力キュー 1 とドロップしきい値 70% のしきい値 ID 2 に割り当てます。

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	WTD しきい値のパーセントを入力キューに割り当てます。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos srr-queue input dscp-map

Differentiated Services Code Point (DSCP) 値を入力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングするには、**mls qos srr-queue input dscp-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。

```
mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue input dscp-map
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

queue <i>queue-id</i>	キュー番号を指定します。 <i>queue-id</i> で指定できる範囲は 1 ~ 2 です。
<i>dscp1...dscp8</i>	DSCP 値を入力キューにマッピングします。 <i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。
threshold <i>threshold-id</i> <i>dscp1...dscp8</i>	DSCP 値をキューのしきい値 ID にマッピングします。 <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。 <i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。

デフォルト

表 2-13 は、デフォルトの DSCP 入力キューしきい値マップを示しています。

表 2-13 デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ~ 39	1-1
40 ~ 47	2-1
48 ~ 63	1-1

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

入力ポートに割り当てられた DSCP によって、入力または出力のキューおよびしきい値が選択されます。

しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。**mls qos srr-queue input threshold** 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、入力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

例

次の例では、DSCP 値 0 ~ 6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。DSCP 値 20 と 26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

設定を確認するには、**show mls qos maps** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input cos-map	サービス クラス (CoS) 値を入力キューにマッピングするか、CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	WTD しきい値のパーセントを入力キューに割り当てます。
show mls qos maps	QoS のマッピング情報を表示します。

mls qos srr-queue input priority-queue

入力プライオリティ キューを設定し、リングが輻輳状態になった場合に内部リング上で帯域幅を保証するには、**mls qos srr-queue input priority-queue** 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。

mls qos srr-queue input priority-queue *queue-id* bandwidth *weight*

no mls qos srr-queue input priority-queue *queue-id*

シンタックスの説明

<i>queue-id</i>	入力キューの ID です。指定できる範囲は 1 ~ 2 です。
bandwidth <i>weight</i>	内部リングの帯域幅のパーセンテージ。指定できる範囲は 0 ~ 40 です。

デフォルト

プライオリティ キューはキュー 2 で、帯域幅の 10% が割り当てられています。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

プライオリティ キューは、優先して進める必要があるトラフィックにのみ使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューは内部リング上で帯域幅の一部が保証されており、オーバーサブスクライプ型のリング上でネットワーク トラフィックが多い場合（バックプレーンが送達できる量よりもトラフィックが多い場合、およびキューが満杯でフレームをドロップしている場合）に、遅延とジッタを軽減します。

シェイプドラウンドロビン (SRR) は、**mls qos srr-queue input priority-queue *queue-id* bandwidth *weight*** グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定された重みに従ってプライオリティ キューにサービスを提供します。SRR は、両方の入力キューで残りの帯域幅を共有し、**mls qos srr-queue input bandwidth *weight1 weight2*** グローバル コンフィギュレーション コマンドで設定されたウェイトで指定しているサービスを行います。

プライオリティ キューイングをディセーブルにするには、帯域幅の重みを **0** に設定します。たとえば、**mls qos srr-queue input priority-queue *queue-id* bandwidth 0** と入力します。

■ mls qos srr-queue input priority-queue

例

次の例では、キューの入力帯域幅を割り当てる方法を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/(4+4) です。SRR は最初、設定された 10% の帯域幅をキュー 1 (プライオリティ キュー) にサービスします。そのあと、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

設定を確認するには、**show mls qos interface [interface-id] queueing** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input cos-map	サービス クラス (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input threshold	Weighted Tail-Drop (WTD) しきい値のパーセントを入力キューに割り当てます。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface queueing	QoS (Quality of Service) 情報を表示します。

mls qos srr-queue input threshold

入力キューに重み付きテール ドロップ (WTD) しきい値 (%) を割り当てるには、**mls qos srr-queue input threshold** 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。

```
mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2
no mls qos srr-queue input threshold queue-id
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>queue-id</i>	入力キューの ID です。指定できる範囲は 1 ~ 2 です。
<i>threshold-percentage1</i>	2 つの WTD しきい値 (%) です。各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。各値はスペースで区切ります。指定できる範囲は 1 ~ 100 です。
<i>threshold-percentage2</i>	

デフォルト

QoS (Quality of Service) がイネーブルなときは、WTD もイネーブルです。
2 つの WTD しきい値は、100% に設定されます。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

QoS は、サービス クラス (CoS) / しきい値マップまたは Differentiated Services Code Point (DSCP) / しきい値マップを使用して、どの CoS 値または DSCP 値をしきい値 1 としきい値 2 にマッピングするかを判別します。しきい値 1 を超えた場合は、しきい値を超えなくなるまで、CoS または DSCP がこのしきい値に割り当てられたパケットがドロップされます。ただし、しきい値 2 に割り当てられたパケットは、2 番めのしきい値を超えることがないかぎり、引き続きキューに入れられ送信されます。
各キューには、2 つの設定可能な (明示) ドロップしきい値と 1 つの事前設定された (暗黙) ドロップしきい値 (フル) があります。

CoS/ しきい値マップを設定するには、**mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用します。DSCP/ しきい値マップを設定するには、**mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、2 つのキューにテールドロップしきい値を設定する方法を示します。キュー 1 のしきい値は 50% と 100%、キュー 2 のしきい値は 70% と 100% です。

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

■ mls qos srr-queue input threshold

設定を確認するには、**show mls qos interface [interface-id] buffers** または **show mls qos input-queue** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input cos-map	サービス クラス (CoS) 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピングするか、DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
show mls qos input-queue	入力キューの設定を表示します。
show mls qos interface buffers	QoS (Quality of Service) 情報を表示します。

mls qos srr-queue output cos-map

サービス クラス (CoS) 値を出力キューにマッピングするか、または CoS 値をキューとしきい値 ID にマッピングするには、**mls qos srr-queue output cos-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。

```
mls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue output cos-map
```

シンタックスの説明

queue <i>queue-id</i>	キュー番号を指定します。 <i>queue-id</i> に指定できる範囲は 1 ~ 4 です。
<i>cos1...cos8</i>	CoS 値を出力キューへマッピングします。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。
threshold <i>threshold-id</i> <i>cos1...cos8</i>	CoS 値をキューのしきい値 ID にマッピングします。 <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。

デフォルト

表 2-14 では、デフォルトの CoS 出力キューのしきい値のマッピングを示します。

表 2-14 デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID - しきい値 ID
0、1	2-1
2、3	3-1
4	4-1
5	1-1
6、7	4-1

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの QoS (Quality of Service) ソリューションを満たさないと判断した場合のみ、設定を変更することができます。

mls qos queue-set output *qset-id* threshold 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、出力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当てることができます。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。CoS 値 0 ~ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50% と 70% に設定し、割り当てられたメモリの 100% を保証 (予約) して、このキューがパケットをドロップせずに保持可能な最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface [*interface-id*] buffers**、または **show mls qos queue-set** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue output dscp-map	Differentiated Service Code Point (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	WTD しきい値を設定して、バッファの可用性を保証し、キューセットへの最大メモリ割り当てを設定します。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface buffers	QoS 情報を表示します。
show mls qos maps	QoS のマッピング情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos srr-queue output dscp-map

Differentiated Services Code Point (DSCP) 値を出力キューにマッピングするか、または DSCP 値をキューとしきい値 ID にマッピングするには、**mls qos srr-queue output dscp-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。

```
mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue output dscp-map
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

queue <i>queue-id</i>	キュー番号を指定します。 <i>queue-id</i> に指定できる範囲は 1 ~ 4 です。
<i>dscp1...dscp8</i>	DSCP 値を出力キューにマッピングします。 <i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。
threshold <i>threshold-id</i> <i>dscp1...dscp8</i>	DSCP 値をキューのしきい値 ID にマッピングします。 <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。 <i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。

デフォルト

表 2-15 は、デフォルトの DSCP 出力キューしきい値マップを示しています。

表 2-15 デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ~ 15	2-1
16 ~ 31	3-1
32 ~ 39	4-1
40 ~ 47	1-1
48 ~ 63	4-1

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱい
の状態に対して設定されます。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したう
えで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してく
ださい。

mls qos queue-set output *qset-id* threshold 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、出力キューに 2 つの Weighted Tail-Drop (WTD) しきい値 (%) を割り当てることができます。

各 DSCP 値を異なるキューおよびしきい値の組み合わせにマッピングして、フレームが別の方法で処
理されるようにすることができます。

コマンドあたり最大 8 個の DSCP 値をマッピングできます。

例

次の例では、ポートをキューセット 1 にマッピングする方法を示します。DSCP 値 0 ~ 3 を出力キュー
1 としきい値 ID 1 にマッピングします。キュー 1 のドロップしきい値を割り当てられたメモリの 50%
と 70% に設定し、割り当てられたメモリの 100% を保証 (予約) して、このキューがパケットをド
ロップせずに保持可能な最大メモリを 200% に設定します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 1
```

設定を確認するには、**show mls qos maps**、**show mls qos interface [*interface-id*] buffers**、または
show mls qos queue-set 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos srr-queue output cos-map	サービス クラス (CoS) 値を出力キュー、またはキューとし きい値 ID にマッピングします。
mls qos queue-set output threshold	WTD しきい値を設定して、バッファのアベイラビリティを 保証し、キューセットへの最大メモリ割り当てを設定します。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface buffers	QoS (Quality of Service) 情報を表示します。
show mls qos maps	QoS のマッピング情報を表示します。
show mls qos queue-set	キューセットの出力キューセット値を表示します。

mls qos trust

ポートの信頼状態を設定するには、**mls 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。入力トラフィックを信頼できるようになり、パケットの Differentiated Service Code Point (DSCP)、サービス クラス (CoS)、または IP precedence のフィールドを調べることにより分類が実行されます。ポートを信頼できない状態に戻すには、このコマンドの **no** 形式を使用します。

mls qos trust [cos | device cisco-phone | dscp | ip-precedence]

no mls qos trust [cos | device | dscp | ip-precedence]

シンタックスの説明

cos	(任意) パケットの CoS 値を使用して、入力パケットを分類します。タグのないパケットについては、ポートのデフォルト CoS 値を使用します。
device cisco-phone	(任意) 信頼設定に応じて、Cisco IP Phone (信頼される境界) から送信された CoS 値または DSCP 値を信頼することにより入力パケットを分類します。
dscp	(任意) パケット DSCP 値 (8 ビット サービスタイプ フィールドの上位 6 ビット) を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグなしパケットの場合は、デフォルトのポート CoS 値が使用されます。
ip-precedence	(任意) パケットの IP precedence 値 (8 ビット サービスタイプ フィールドの上位 3 ビット) を使用して、入力パケットを分類します。非 IP パケットでパケットがタグ付きの場合は、パケット CoS が使用されます。タグのないパケットの場合、デフォルト ポートの CoS 値が使用されます。

デフォルト

ポートは信頼されていません。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

QoS (Quality of Service) ドメインに着信するパケットは、ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートはいずれか 1 つの信頼状態に設定できます。ポートが信頼されているかどうか、またどのパケットのフィールドがトラフィックの分類に使用されるのかを指定する場合には、このコマンドを使用します。

ポートに信頼 DSCP または信頼 IP precedence が設定され、着信パケットが非 IP パケットの場合は、CoS/DSCP マップを使用して、CoS 値から対応する DSCP 値が導き出されます。CoS は、トランクポートの場合はパケット CoS、非トランクポートの場合はデフォルトのポート CoS となります。

DSCP が信頼されている場合、IP パケットの DSCP フィールドは変更されません。ただし、パケットの CoS 値を (DSCP/CoS マップに基づいて) 変更することは可能です。

CoS が信頼されている場合、パケットの CoS フィールドは変更されませんが、IP パケットである場合には (CoS/DSCP マップに基づいて) DSCP を変更することはできません。

信頼境界機能は、ユーザがネットワーク化された Cisco IP Phone から PC を切断し、これをスイッチポートに接続して信頼された CoS または DSCP 設定を利用する場合のセキュリティ問題の発生を防止します。スイッチおよび IP Phone に接続されたポートで Cisco Discovery Protocol (CDP) をグローバルにイネーブルにする必要があります。IP Phone が検出されなかった場合、信頼境界機能はスイッチまたはルーテッドポートの信頼設定をディセーブルにし、高プライオリティ キューが誤って使用されないようにします。

DSCP または IP precedence の信頼設定を行うと、着信パケットの DSCP 値または IP precedence 値が信頼されます。IP Phone に接続するスイッチポートで **mls qos cos override** インターフェイス コンフィギュレーション コマンドを設定すると、スイッチは着信音声およびデータパケットの CoS を無効にし、デフォルトの CoS 値をそれらに割り当てます。

QoS ドメイン間境界の場合は、ポートを DSCP 信頼状態に設定し、DSCP 値が QoS ドメイン間で異なる場合は DSCP/DSCP 変換マップを適用することができます。

ポート信頼状態を使用した分類 (たとえば、**mls qos trust [cos | dscp | ip-precedence]**) とポリシーマップ (たとえば、**service-policy input policy-map-name**) は同時に指定できません。最後に行われた設定により、前の設定が上書きされます。

例

次の例では、着信パケットの IP precedence フィールドを信頼するようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust ip-precedence
```

次の例では、ポートに接続されている Cisco IP Phone が信頼できるデバイスになるように指定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust device cisco-phone
```

設定を確認するには、**show mls qos interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos cos	デフォルトのポート CoS 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てます。
mls qos dscp-mutation	DSCP/DSCP 変換マップを DSCP の信頼できるポートに適用します。
mls qos map	CoS/DSCP マップ、DSCP/CoS マップ、DSCP/DSCP 変換マップ、IP precedence/DSCP マップ、およびポリシー設定 DSCP マップを定義します。
show mls qos interface	QoS 情報を表示します。

monitor session

新規の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/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 センサー アプライアンスなど) の宛先ポート上で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や VLAN を追加/削除し、SPAN 送信元トラフィックを特定の VLAN に制限 (フィルタリング) するには、**monitor session** 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/宛先のインターフェイスやフィルタを削除したりする場合は、このコマンドの **no** 形式を使用します。宛先インターフェイスに対してこのコマンドの **no** 形式を使用すると、カプセル化オプションは無視されます。

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation
{dot1q | replicate}]} [ingress {dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id}]
| {remote vlan vlan-id}
```

```
monitor session session_number filter vlan vlan-id [, | -]
```

```
monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan
vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

```
no monitor session {session_number | all | local | remote}
```

```
no monitor session session_number destination {interface interface-id [, | -] [encapsulation
{dot1q | replicate}]} [ingress {dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id}]
| {remote vlan vlan-id}
```

```
no monitor session session_number filter vlan vlan-id [, | -]
```

```
no monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} |
{vlan vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

シンタックスの説明

<i>session_number</i>	SPAN または RSPAN セッションで識別されるセッション番号を指定します。指定できる範囲は 1 ~ 66 です。
destination	SPAN または RSPAN の宛先を指定します。宛先は物理ポートである必要があります。
interface <i>interface-id</i>	SPAN または RSPAN セッションの宛先または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 (タイプおよびポート番号を含む) 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 ~ 6 です。
encapsulation dot1q	(任意) 宛先インターフェイスが IEEE 802.1Q カプセル化方式を使用することを指定します。 次のキーワードは、ローカル SPAN にのみ有効です。RSPAN に対しては、RSPAN VLAN ID が元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。
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のカプセル化方式を複製することを指定します。 次のキーワードは、ローカル SPAN にのみ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。

ingress	(任意) 入トラフィック転送をイネーブルにします。
dot1q vlan vlan-id	デフォルト VLAN として指定された VLAN で IEEE 802.1Q カプセル化を持つ着信パケットを受け入れます。
untagged vlan vlan-id	デフォルト VLAN として指定された VLAN でタグなしカプセル化を持つ着信パケットを受け入れます。
vlan vlan-id	ingress キーワードのみで使用された場合、入トラフィックにデフォルトの VLAN を設定します。
remote vlan vlan-id	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 および 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。
,	(任意) 一連のインターフェイスまたは VLAN を指定します。または、以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。
filter vlan vlan-id	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとして VLAN のリストを指定します。vlan-id で指定できる範囲は 1 ~ 4094 です。
source	SPAN または RSPAN の送信元を指定します。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。
both、rx、tx	(任意) 監視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。
source vlan vlan-id	SPAN の送信元インターフェイスを VLAN ID として指定します。指定できる範囲は 1 ~ 4094 です。
all、local、remote	すべての SPAN および RSPAN、すべてのローカル SPAN、すべての RSPAN セッションをクリアするため、 no monitor session コマンドに all、local、remote を指定します。 all キーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。

デフォルト

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監視します。

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 が監視されます。

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。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 を使用して監視できます。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監視できません。

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチ上で、合計 66 の SPAN および RSPAN セッションを保有できます。

スイッチ上で、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、監視された VLAN ID のパケットのみ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監視できます。[,|-] オプションを使用することにより、一連のインターフェイスまたはインターフェイス範囲、一連の VLAN または VLAN 範囲を指定します。

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 ポートは、SPAN または RSPAN 宛先ポートとして設定することはできません。EtherChannel グループのメンバー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。

個々のポートはそれらが EtherChannel に参加している間も監視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 バンドル全体を監視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 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せんが、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。

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監視されます。**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。

入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。

- 他のキーワードなしで、**monitor session session_number destination interface interface-id** を入力した場合、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後続くキーワードが **dot1q**、**untagged** のいずれであるかによって決まります。
- 他のキーワードを指定せずに **monitor session session_number destination interface interface-id encapsulation dot1q** を入力すると、出力カプセル化で IEEE 802.1Q カプセル化方式が使用されます。(これは、ローカル SPAN だけに適用されます。RSPAN は **dot1q カプセル化** をサポートしていません)。
- **monitor session session_number destination interface interface-id encapsulation dot1q ingress** を入力した場合は、出力カプセル化には IEEE 802.1Q カプセル化が使用され、入力カプセル化はその後続くキーワードが、**dot1q** または **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 だけに適用されます。RSPAN は **dot1q カプセル化** をサポートしていません)。
- その他のキーワードを指定せずに、**monitor session session_number destination interface interface-id encapsulation replicate** 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、入力トラフィック転送はイネーブルにはなりません。(これはローカル SPAN のみに適用します。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のカプセル化を複製し、入力カプセル化はその後続くキーワードが、**dot1q**、**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 のみに適用します。RSPAN はカプセル化の複製をサポートしていません)。

例

次の例では、ローカル SPAN セッション 1 を作成し、送信元ポート 1 から宛先ポート 2 に送受信するトラフィックを監視する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

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。

```
Switch(config)# no monitor session 2 destination gigabitethernet0/2
```

次の例では、既存のセッションの SPAN トラフィックを特定の VLAN にのみ制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次の例では、複数の送信元インターフェイスを監視する 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 gigabitethernet0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

次の例では、監視されたトラフィックを受信するスイッチで RSPAN 宛先セッション 10 を設定する方法を示します。

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet0/2
```

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。

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation replicate 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、タグ付けされていません。

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress untagged vlan 5
```

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 および RSPAN 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。

関連コマンド

コマンド	説明
remote-span	vlan コンフィギュレーション モードで RSPAN VLAN を設定します。
show monitor	SPAN および RSPAN セッション情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

mvr (グローバル コンフィギュレーション)

スイッチ上で Multicast VLAN Registration (MVR) 機能をイネーブルにするには、キーワードを指定せずに **mvr** 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。このコマンドをキーワードとともに使用すると、スイッチの MVR モードの設定、MVR IP マルチキャストアドレスの設定、またはグループ メンバシップからのポートの削除を行う前に、クエリーの返答を待つ最大時間の設定、または MVR マルチキャスト VLAN の指定が行われます。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。

```
mvr [group ip-address [count] | mode [compatible | dynamic] | querytime value | vlan
vlan-id]
```

```
no mvr [group ip-address | mode [compatible | dynamic] | querytime value | vlan vlan-id]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

group ip-address	スイッチ上で MVR グループ IP マルチキャスト アドレスをスタティックに設定します。 スタティックに設定した IP マルチキャスト アドレスまたは連続アドレスを削除したり、IP アドレスが入力されない場合にすべてのスタティックに設定された MVR IP マルチキャスト アドレスを削除したりする場合は、このコマンドの no 形式を使用します。
count	(任意) 複数の連続 MVR グループ アドレスを設定します。指定できる範囲は 1 ~ 256 です。デフォルト値は 1 です。
mode	(任意) MVR の動作モードを指定します。 デフォルトは compatible モードです。
compatible	MVR モードを設定して、Catalyst 2900 XL および Catalyst3500XL スイッチと互換性を持つようにします。このモードでは、送信元ポートでのダイナミック メンバシップ加入は使用できません。
dynamic	MVR モードを設定して、送信元ポートでダイナミック MVR メンバシップを使用できるようにします。
querytime value	(任意) レシーバー ポートで IGMP レポート メンバシップを待機する最大時間を設定します。この時間は、レシーバー ポート脱退処理にだけ適用されます。IGMP クエリーがレシーバー ポートから送信された場合、スイッチは、デフォルトまたは設定された MVR クエリー時間が経過するまで IGMP グループ メンバシップ レポートを待ってから、ポートをマルチキャスト グループ メンバシップから削除します。 この値は 10 分の 1 秒単位の応答時間です。指定できる範囲は 1 ~ 100 です。デフォルトは 5/10 秒つまり 1/2 秒です。 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 vlan-id	(任意) MVR マルチキャスト データの受信が予想される VLAN を指定します。これは、すべての送信元ポートが属する VLAN でもあります。指定できる範囲は 1 ~ 4094 です。デフォルト値は VLAN 1 です。

デフォルト

MVR はデフォルトでディセーブルです。

デフォルトの MVR モードは、**compatible** モードです。

IP マルチキャスト アドレスは、デフォルトではスイッチで設定されます。

デフォルトのグループ IP アドレス カウントは **0** です。

デフォルトのクエリー応答時間は **5/10** 秒すなわち **1/2** 秒です。

MVR 用のデフォルト マルチキャスト VLAN は **VLAN 1** です。

コマンドモード グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

1 つのスイッチ上で最大 **256** の MVR マルチキャスト グループを設定できます。

MVR に属するすべての IP マルチキャスト アドレスをスタティックに設定する場合は、**mvr group** コマンドを使用します。設定したマルチキャスト アドレスに送信されたマルチキャスト データは、スイッチのすべての送信元ポートおよびその IP マルチキャスト アドレスでデータを受信するよう登録されたすべてのレシーバー ポートに送信されます。

MVR はスイッチ上でエイリアス IP マルチキャスト アドレスをサポートしています。ただし、スイッチが **Catalyst 3550** または **Catalyst 3500 XL** スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス (**224.0.0.xxx** 範囲内) を設定する必要はありません。

mvr querytime コマンドはレシーバー ポートだけに適用されます。

スイッチ MVR が、**Catalyst 2900 XL** または **Catalyst 3500 XL** スイッチと相互動作している場合は、マルチキャスト モードを **compatible** に設定してください。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

MVR はスイッチで IGMP スヌーピングと共存できます。

例

次の例では、MVR をイネーブルにする方法を示します。

```
Switch(config)# mvr
```

show mvr 特権 EXEC コマンドを使用すると、最大のマルチキャスト グループの現在の設定を表示できます。

次の例では、**228.1.23.4** を IP マルチキャスト アドレスとして設定する方法を示します。

```
Switch(config)# mvr group 228.1.23.4
```

次の例では、**228.1.23.1 ~ 228.1.23.10** のマルチキャスト アドレスとともに **10** の連続 IP マルチキャスト グループを設定する方法を示します。

```
Switch(config)# mvr group 228.1.23.1 10
```

スイッチで設定された IP マルチキャスト グループ アドレスを表示する場合は、**show mvr members** 特権 EXEC コマンドを使用します。

■ mvr (グローバル コンフィギュレーション)

次の例では、最大クエリ応答時間を 1 秒 (10/10) に設定する方法を示します。

```
Switch(config)# mvr querytime 10
```

次の例では、VLAN 2 をマルチキャスト VLAN として設定する方法を示します。

```
Switch(config)# mvr vlan 2
```

設定を確認するには、**show mvr** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mvr (インターフェイス コンフィギュレーション)	MVR ポートを設定します。
show mvr	MVR グローバルパラメータまたはポートパラメータを表示します。
show mvr interface	設定された MVR インターフェイスをそのタイプ、ステータス、および即時脱退設定とともに表示します。インターフェイスがメンバーであるすべての MVR グループを表示します。
show mvr members	MVR マルチキャストグループのメンバーであるすべてのポートを表示します。グループにメンバーがない場合、そのステータスは Inactive として表示されます。

mvr (インターフェイス コンフィギュレーション)

レイヤ 2 ポートを Multicast VLAN Registration (MVR) のレシーバー ポートまたは送信元ポートとして設定し、即時脱退機能を設定し、IP マルチキャスト VLAN と IP アドレスにポートをスタティックに割り当てるには、**mvr** 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。

```
mvr [immediate | type {receiver | source} | vlan vlan-id group [ip-address]]
```

```
no mvr [immediate | type {source | receiver} | vlan vlan-id group [ip-address]]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

immediate	(任意) ポート上で MVR の即時脱退機能をイネーブルにします。この機能をディセーブルにするには、 no mvr immediate コマンドを使用します。
type	(任意) ポートを MVR レシーバー ポートまたは送信元ポートとして設定します。 デフォルト ポート タイプは、MVR 送信元ポートおよびレシーバーポートのどちらでもありません。 no mvr type コマンドは、送信元ポートおよびレシーバー ポートのどちらでもないポートとしてポートをリセットします。
receiver	ポートを、マルチキャスト データの受信のみが可能な加入者ポートとして設定します。レシーバー ポートはマルチキャスト VLAN に属することはできません。
source	ポートを、設定済みのマルチキャスト グループとのマルチキャスト データの送受信が可能なアップリンク ポートとして設定します。スイッチのポートはすべて単一のマルチキャスト VLAN に属します。
vlan <i>vlan-id</i> group	(任意) ポートを、指定された VLAN ID を持つマルチキャストグループのスタティック メンバーとして追加します。 no mvr vlan <i>vlan-id</i> group コマンドは、IP マルチキャスト アドレス グループのメンバシップから VLAN 上のポートを削除します。
<i>ip-address</i>	(任意) 指定されたマルチキャスト VLAN ID の指定された MVR IP マルチキャスト グループ アドレスをスタティックに設定します。これは、ポートが加入しているマルチキャストグループの IP アドレスです。

デフォルト

ポートはレシーバーとしても送信元としても設定されません。

即時脱退機能はすべてのポートでディセーブルです。

レシーバー ポートはどの設定済みマルチキャスト グループにも属していません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ポートが設定されたマルチキャスト グループ向けマルチキャスト データを送受信できるようにする場合は、ポートを送信元ポートとして設定します。マルチキャスト データは送信元ポートとして設定されているすべてのポートで受信されます。

レシーバー ポートはトランク ポートになることはできません。スイッチのレシーバー ポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。

MVR に参加していないポートは、MVR レシーバー ポートまたは送信元ポートとして設定しないでください。非 MVR ポートは通常のスイッチ ポートであり、通常のスイッチ動作でマルチキャスト データを送受信することができます。

即時脱退機能がイネーブルの場合、レシーバー ポートはより短時間でマルチキャスト グループから脱退します。即時脱退機能がなく、スイッチがレシーバー ポートのグループから IGMP Leave メッセージを受信した場合、スイッチは、そのポートに IGMP MAC (メディア アクセス制御) ベースのクエリーを送信し、IGMP グループ メンバシップ レポートを待ちます。設定された時間内にレポートが届かないと、レシーバー ポートがマルチキャスト グループ メンバシップから削除されます。即時脱退機能では、IGMP Leave を受信したレシーバー ポートから IGMP MAC ベースのクエリーは送信されません。Leave メッセージの受信後ただちに、マルチキャスト グループ メンバシップからレシーバー ポートが削除されるので、脱退のための待ち時間が短縮されます。

即時脱退機能をイネーブルにするのは、レシーバー装置が 1 つだけ接続されているレシーバー ポートに限定してください。

mvr vlan group コマンドは、IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するようにポートをスタティックに設定します。グループのメンバーとしてスタティックに設定されたポートは、スタティックに削除されるまではそのグループのメンバーのままです。compatible モードでは、このコマンドはレシーバー ポートだけに適用されます。dynamic モードでは送信元ポートにも適用されます。レシーバー ポートは、IGMP Join メッセージを使用してダイナミックにマルチキャスト グループに加入することもできます。

compatible モードで動作している場合は、MVR は MVR 送信元ポートでの IGMP ダイナミック加入をサポートしません。

例

次の例では、MVR レシーバー ポートとしてポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr type receiver
```

設定されたレシーバー ポートおよび送信元ポートを表示するには、**show mvr interface** 特権 EXEC コマンドを使用します。

次の例では、ポートの即時脱退機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr immediate
```

次の例では、VLAN 1 のポートを IP マルチキャスト グループ 228.1.23.4 のスタティック メンバーとして追加する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

設定を確認するには、**show mvr members** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>mvr</code> (グローバル コンフィギュレーション)	スイッチ上で MVR をイネーブルにして、設定します。
<code>show mvr</code>	MVR グローバル パラメータまたはポート パラメータを表示します。
<code>show mvr interface</code>	設定済みの MVR インターフェイスを表示するか、またはレシーバー ポートが所属するマルチキャスト グループを表示します。インターフェイスがメンバーであるすべての MVR グループを表示します。
<code>show mvr members</code>	MVR マルチキャスト グループに属するすべてのレシーバー ポートを表示します。

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、**network-policy** インターフェイス コンフィギュレーション コマンドを使用します。ポリシーを削除する場合は、このコマンドの **no** 形式を使用します。

network-policy *profile number*

no network-policy



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>profile number</i>	ネットワーク ポリシー プロファイル番号を指定します。
-----------------------	-----------------------------

デフォルト

ネットワーク ポリシー プロファイルが適用されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

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。

インターフェイスに初めてネットワーク ポリシー プロファイルを適用する場合は、そのインターフェイス上で **switchport voice vlan** コマンドを設定できません。インターフェイス上で **switchport voice vlan** *vlan-id* がすでに設定されている場合は、その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できます。そのインターフェイスに音声 VLAN または音声信号 VLAN のネットワーク ポリシー プロファイルが適用されます。

例

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。

```
Switch(config)# interface_id
Switch(config-if)# network-policy profile 60
```

関連コマンド

コマンド	説明
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ます。
network-policy profile (ネット ワーク ポリシー コンフィギュレ ーション)	ネットワーク ポリシー プロファイルの属性を設定します。
show network-policy profile	設定されたネットワーク ポリシー プロファイルを表示します。

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 ポリシー設定モードを開始する ... 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。既存のポリシーを削除し、グローバル コンフィギュレーション モードに戻る場合は、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*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>profile number</i>	ネットワーク ポリシー プロファイル番号を指定します。指定できる範囲は 1 ~ 4294967295 です。
-----------------------	--

デフォルト

ネットワーク ポリシー プロファイルが定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

プロファイルを作成し、ネットワーク ポリシー プロファイル設定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 プロファイル設定モードから特権 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 プロファイル設定モードに入っている場合は、VLAN、サービス クラス (CoS)、Differentiated Services Code Point (DSCP)、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。

この後、これらのプロファイル属性が Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) **network-policy** Type-Length-Value (TLV) に格納されます。

例

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。

```
Switch(config)# network-policy profile 60
Switch(config-network-policy)#
```


関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
network-policy profile (ネットワーク ポリシー コンフィギュレーション)	ネットワーク ポリシー プロファイルの属性を設定します。
show network-policy profile	設定されたネットワーク ポリシー プロファイルを表示します。

network-policy profile (ネットワーク ポリシー コンフィギュレーション)

network-policy profile グローバル コンフィギュレーション コマンドでネットワーク ポリシー プロファイルを設定するには、**network-policy profile** コンフィギュレーション モード コマンドを使用します。プロファイルを削除する場合は、追加パラメータを指定せずにこのコマンドの **no** 形式を使用します。設定された属性を変更する場合は、パラメータを指定してこのコマンドの **no** 形式を使用します。

```
network-policy profile profile number {voice | voice-signaling} vlan [vlan-id {cos cvalue | dscp dvalue}] | [[dot1p {cos cvalue | dscp dvalue}] | none | untagged]
```

```
no network-policy profile profile number {voice | voice-signaling} vlan [vlan-id | {cos cvalue} | {dscp dvalue}] | [[dot1p {cos cvalue} | {dscp dvalue}] | none | untagged]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

voice	音声アプリケーション タイプを指定します。
voice-signaling	音声信号アプリケーション タイプを指定します。
vlan	音声トラフィック用のネイティブ VLAN を指定します。
<i>vlan-id</i>	(任意) 音声トラフィック用の VLAN を指定します。指定できる範囲は 1 ~ 4094 です。
<i>cos cvalue</i>	(任意) 設定された VLAN のレイヤ 2 プライオリティ サービス クラス (CoS) を指定します。指定できる範囲は 0 ~ 7 であり、デフォルト値は 0 です。
<i>dscp dvalue</i>	(任意) 設定された VLAN の Differentiated Services Code Point (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 であり、デフォルト値は 0 です。
dot1p	(任意) IEEE 802.1p プライオリティ タギングと VLAN 0 (ネイティブ VLAN) を使用するように IP Phone を設定します。
none	(任意) 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	(任意) 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。

デフォルト

ネットワーク ポリシーが定義されていません。

コマンドモード

ネットワーク ポリシー コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

ネットワーク ポリシー プロファイルの属性を設定するには、**network-policy profile** コマンドを使用します。

voice アプリケーション タイプは、対話形式の音声サービスをサポートしている専用 IP Phone およびそれと同等のデバイスを対象としています。通常、これらのデバイスは、導入の簡素化とセキュリティの強化を図るために、データ アプリケーションから切り離して別々の VLAN 上に配置されます。

voice-signaling アプリケーション タイプは、音声信号と音声メディアにそれぞれ異なるポリシーが必要となるネットワーク トポロジを対象としています。すべてのネットワーク ポリシーが **voice policy TLV** でアドバタイズされたものとして適用されている場合は、このアプリケーション タイプをアドバタイズしないでください。

次の例では、プライオリティ 4 CoS の VLAN 100 に対して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。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)#voice vlan 100 cos 4
```

次の例では、DSCP 値 34 の VLAN 100 に対して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。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 dscp 34
```

次の例では、プライオリティ タギングを使用したネイティブ VLAN に対して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。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
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ます。
show network-policy profile	設定されたネットワーク ポリシー プロファイルを表示します。

nmsp

スイッチ上でネットワーク モビリティ サービス プロトコル (NMSP) をイネーブルにするには、**nmsp global configuration** コマンドを使用します。このコマンドを使用できるのは、スイッチで暗号化ソフトウェア イメージが実行されている場合だけです。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。

nmsp {enable | {notification interval {attachment | location} interval-seconds}}

no nmsp {enable | {notification interval {attachment | location} interval-seconds}}



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

enable	スイッチ上で NMSP 機能をイネーブルにします。
notification interval	NMSP 通知間隔を指定します。
attachment	接続通知間隔を指定します。
location	位置通知間隔を指定します。
interval-seconds	スイッチから MSE に位置更新または接続更新が送信されるまでの期間 (秒)。指定できる範囲は 1 ~ 30 であり、デフォルト値は 30 です。

デフォルト

NMSP がディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

スイッチから Cisco Mobility Services Engine (MSE; モビリティ サービス エンジン) への NMSP 位置通知および接続通知の送信をイネーブルにするには、**nmsp** 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。

例

次の例では、スイッチ上で NMSP をイネーブルにして、位置通知間隔を 10 秒に設定する方法を示します。

```
Switch(config)#nmsp enable
Switch(config)#nmsp notification interval location 10
```

関連コマンド

コマンド	説明
<code>clear nmsp statistics</code>	NMSP 統計カウンタをクリアします。
<code>nmsp attachment suppress</code>	指定されたインターフェイスからの接続情報のレポートを抑制します。
<code>show nmsp</code>	NMSP 情報を表示します。

nmsp attachment suppress

指定されたインターフェイスからの接続情報のレポートを抑制するには、**nmsp attachment suppress** 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。このコマンドを使用できるのは、スイッチで暗号化ソフトウェア イメージが実行されている場合だけです。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。

nmsp attachment suppress

no nmsp attachment suppress



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

Cisco モビリティ サービス エンジン (MSE) に位置通知と接続通知を送信ないようにインターフェイスを設定するには、**nmsp attachment suppress** 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。

例

次の例では、MSE に接続情報を送信ないようにインターフェイスを設定する方法を示します。

```
Switch(config)# switch interface interface-id
Switch(config-if)# nmsp attachment suppress
```

関連コマンド

コマンド	説明
nmsp	スイッチ上で Network Mobility Services Protocol (NMSP) をイネーブルにします。
show nmsp	NMSP 情報を表示します。

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、**pagp learn-method** 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。

pagp learn-method {aggregation-port | physical-port}

no pagp learn-method

シンタックスの説明

aggregation-port	論理ポート チャンネルで学習するアドレスを指定します。スイッチは、EtherChannel のいずれかのポートを使用することによって、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 内の物理ポートで学習するアドレスを指定します。スイッチは、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。チャンネルの一方の終端は、特定の宛先 MAC (メディア アクセス制御) または IP アドレスのチャンネルのポートと同一のポートを使用します。

デフォルト

aggregation-port (論理ポート チャンネル) です。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。



(注)

CLI (コマンドライン インターフェイス) を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習のみです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効になっていますが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習のみをサポートしているデバイスとの PAgP の相互運用のためにこれらのコマンドが必要となります。

スイッチへのリンク パートナーが物理ラーナーの場合、**pagp learn-method physical-port** 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イッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** 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送信元 MAC アドレスに基づく負荷分散方式を設定することを推奨します。この状況でのみ、**pagp learn-method** 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。

例

次の例では、学習方式を設定し、EtherChannel 内の物理ポート上のアドレスを学習する方法を示します。

```
Switch(config-if)# pagp learn-method physical-port
```

次の例では、学習方法を設定し、EtherChannel 内のポート チャンネル上のアドレスを学習する方法を示します。

```
Switch(config-if)# pagp learn-method aggregation-port
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp channel-group-number internal** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
pagp port-priority	EtherChannel を経由するすべてのトラフィックが送信されるポートを選択します。
show pagp	PAgP チャンネル グループ情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

pagp port-priority

EtherChannel 経由のすべてのポート集約プロトコル (PAgP) トラフィックが送信されるポートを選択するには、**pagp port-priority** 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。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動状態にできます。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。

pagp port-priority priority

no pagp port-priority

シンタックスの説明

priority プライオリティ番号の範囲は 0 ~ 255 です。

デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

同じ EtherChannel 内で動作可能でメンバ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。



(注)

CLI (コマンドライン インターフェイス) を経由して **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは、集約ポートでのアドレスの学習のみです。スイッチ ハードウェアでは、**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは無効になっていますが、Catalyst 1900 スイッチなどの物理ポートによるアドレス学習のみをサポートしているデバイスとの PAgP の相互運用のためにこれらのコマンドが必要となります。

スイッチへのリンク パートナーが物理ラーナーの場合、**pagp learn-method physical-port** 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イッチを物理ポート ラーナーとして設定し、**port-channel load-balance src-mac** 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送信元 MAC アドレスに基づく負荷分散方式を設定することを推奨します。この状況でのみ、**pagp learn-method** 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。

例

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。

```
Switch(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp channel-group-number internal** 特権 EXEC コマンドを入力します。

■ pagp port-priority

関連コマンド

コマンド	説明
pagp learn-method	着信パケットの送信元アドレスを学習する機能を提供します。
show pagp	PAgP チャンネル グループ情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。

permit (ARP アクセス リスト コンフィギュレーション)

Dynamic Host Configuration Protocol (DHCP) バインディングの照合条件と一致したアドレス解決プロトコル (ARP) パケットを許可するには、**permit** ARP アクセス リスト コンフィギュレーション コマンドを使用します。指定したアクセス コントロール エントリ (ACE) をアクセス コントロール リストから削除する場合は、このコマンドの **no** 形式を使用します。

```
permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
```

```
no permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
```

シンタックスの説明

request	(任意) ARP 要求の照合条件を指定します。 request を指定しないと、すべての ARP パケットに対して照合が実行されます。
ip	送信元 IP アドレスを指定します。
any	任意の IP アドレスまたは MAC アドレスを受け入れます。
host sender-ip	指定された送信元 IP アドレスを受け入れます。
sender-ip sender-ip-mask	指定された範囲の送信元 IP アドレスを受け入れます。
mac	送信元 MAC アドレスを指定します。
host sender-mac	指定された送信元 MAC アドレスを受け入れます。
sender-mac sender-mac-mask	指定された範囲の送信元 MAC アドレスを受け入れます。
response ip	ARP 応答の IP アドレス値を定義します。
host target-ip	(任意) 指定された宛先 IP アドレスを受け入れます。
target-ip target-ip-mask	(任意) 指定された範囲の宛先 IP アドレスを受け入れます。
mac	ARP 応答の MAC アドレス値を定義します。
host target-mac	(任意) 指定された宛先 MAC アドレスを受け入れます。
target-mac target-mac-mask	(任意) 指定された範囲の宛先 MAC アドレスを受け入れます。
log	(任意) ACE と一致したパケットをロギングします。 ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで matchlog キーワードを設定した場合は、照合条件と一致したパケットがロギングされます。

デフォルト

デフォルト値は設定されていません。

■ permit (ARP アクセス リスト コンフィギュレーション)

コマンド モード ARP アクセス リスト コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン permit 句を追加すると、いくつかの照合条件に基づいて ARP パケットを転送できます。

例 次の例では、ARP アクセス リストを定義し、IP アドレス 1.1.1.1 および MAC アドレス 0000.0000.abcd のホストからの ARP 要求と ARP 応答をいずれも許可する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

設定を確認するには、**show arp access-list** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	arp access-list	ARP アクセス コントロール リスト (ACL) を定義します。
	deny (ARP アクセス リスト コンフィギュレーション)	DHCP バインディングと一致した ARP パケットを拒否します。
	ip arp inspection filter vlan	スタティック IP アドレスが設定されたホストからの ARP 要求と ARP 応答を許可します。
	show arp access-list	ARP アクセス リストの詳細を表示します。

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、**permit** MAC アクセス リスト コンフィギュレーション コマンドを使用します。許可条件を拡張 MAC アクセス リストから削除するには、このコマンドの **no** 形式を使用します。

```
{permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr
| dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]

no {permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host
dst-MAC-addr | dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning
| decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。



(注) **appletalk** は、コマンドラインのヘルプ ストリングには表示されていますが、一致条件としてはサポートされていません。

シンタックスの説明

any	あらゆる送信元または宛先 MAC アドレスを拒否するために指定するキーワードです。
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 マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP 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 マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP 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、Ethernet II または Subnetwork Access Protocol (SNAP) カプセル化を使用して、パケットのプロトコルを識別します。 <ul style="list-style-type: none"> type には、0 ~ 65535 の 16 進数を指定できます。 mask は、マッチングを行う前に Ethertype に適用される <i>don't care</i> ビットのマスクです。
aarp	(任意) データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を選択します。
amber	(任意) EtherType DEC-Amber を選択します。
cos cos	(任意) プライオリティを設定するため、0 ~ 7 までの任意のサービス クラス (CoS) 値を選択します。CoS に基づくフィルタリングは、ハードウェアでのみ実行可能です。 cos オプションが設定されているかどうかを確認する警告メッセージが表示されます。
dec-spanning	(任意) EtherType Digital Equipment Corporation (DEC) スパニング ツリーを選択します。

■ permit (MAC アクセス リスト コンフィギュレーション)

decnet-iv	(任意) EtherType DECnet Phase IV プロトコルを選択します。
diagnostic	(任意) EtherType DEC-Diagnostic を選択します。
dsm	(任意) EtherType DEC-DSM を選択します。
etype-6000	(任意) EtherType 0x6000 を選択します。
etype-8042	(任意) EtherType 0x8042 を選択します。
lat	(任意) EtherType DEC-LAT を選択します。
lavec-sca	(任意) EtherType DEC-LAVC-SCA を選択します。
lsap <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と 802.2 カプセル化を使用して、パケットのプロトコルを識別します。 <i>mask</i> は、マッチングを行う前に LSAP 番号に適用される <i>don't care</i> ビットのマスクです。
mop-console	(任意) EtherType DEC-MOP Remote Console を選択します。
mop-dump	(任意) EtherType DEC-MOP Dump を選択します。
msdos	(任意) EtherType DEC-MSDOS を選択します。
mumps	(任意) EtherType DEC-MUMPS を選択します。
netbios	(任意) EtherType DEC-Network Basic Input/Output System (NETBIOS) を選択します。
vines-echo	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) を選択します。
vines-ip	(任意) EtherType VINES IP を選択します。
xns-idp	(任意) EtherType Xerox Network Systems (XNS) プロトコルスイートを選択します。

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。表 2-16 に、Novell 用語と Cisco IOS 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一覧表示します。

表 2-16 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

デフォルト

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。

コマンドモード

MAC アクセス リスト コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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は、リストの末尾に暗黙的な **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。

名前付き MAC 拡張アクセス リストの詳細については、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。

例

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。

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

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。

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、EtherType 0x4321 のすべてのパケットを許可します。

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

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。

関連コマンド

コマンド	説明
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るのを拒否します。
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
show access-lists	スイッチに設定された ACL を表示します。

police

分類したトラフィックにポリサーを定義するには、**police** ポリシー マップ コンフィギュレーション コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。既存のポリサーを削除するには、このコマンドの **no** 形式を使用します。

police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]

no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>rate-bps</i>	平均トラフィック伝送速度をビット/秒 (b/s) で指定します。指定できる範囲は 1000000 ~ 1000000000 です。
<i>burst-byte</i>	通常のバーストサイズ (バイト) を指定します。指定できる範囲は 8000 ~ 1000000 です。
exceed-action drop	(任意) 指定された伝送速度を超えた場合は、スイッチがパケットをドロップするように指定します。
exceed-action policed-dscp-transmit	(任意) 指定された伝送速度を超えた場合、スイッチがパケットの Differentiated Service Code Point (DSCP) をポリシング設定 DSCP マップに指定された値に変え、パケットを送信するように指定します。

デフォルト

ポリサーは定義されません。

コマンドモード

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

階層ポリシーマップを設定する場合、セカンダリ インターフェイス レベルのポリシーマップで使用できるのは **police** ポリシーマップ コマンドだけです。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー (255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー) をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるといった保証はありません。

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。

ポリシングはトークンバケット アルゴリズムを使用します。バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *burst-byte* オプションまたは **mls qos aggregate-policer** 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。トークンがバケットから削除される速度（平均速度）を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドの *rate-bps* オプションまたは **mls qos aggregate-policer** 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。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。

例

次の例では、トラフィックがバースト サイズ 20 KB で平均伝送速度 1 Mb/s を超えた場合に、ポリサーがパケットをドロップするように設定する方法を示します。着信パケットの DSCP が信頼され、パケットは変更されません。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
```

次の例では、DSCP 値をポリシング設定 DSCP マップに定義された値でマークダウンしてパケットを送信するポリサーを設定する方法を示します。

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# 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。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件 (police 、 set 、および trust ポリシーマップ クラス コンフィギュレーション コマンドによる) を定義します。
mls qos map policed-dscp	ポリシング設定 DSCP マップを DSCP の信頼できるポートに適用します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー マップを作成または変更します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	QoS (Quality Of Service) ポリシー マップを表示します。
trust	class ポリシーマップ コンフィギュレーション コマンドまたは class-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分類されたトラフィックの信頼状態を定義します。

police aggregate

同一のポリシー マップにある複数のクラスにアグリゲート ポリサーを適用するには、**police aggregate** 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。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。指定されたポリサーを削除するには、このコマンドの **no** 形式を使用します。

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

aggregate-policer-name 集約ポリサーの名前です。

デフォルト

集約ポリサーは定義されません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

2 つ以上の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるといった保証はありません。

集約ポリサー パラメータを設定するには、**mls qos aggregate-policer** 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。集約ポリサーは同じポリシー マップ内の複数のクラスに適用されます。異なるポリシー マップにまたがって集約ポリサーを使用することはできません。

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。

階層ポリシーマップで集約ポリサーを設定することはできません。

例 次の例では、集約ポリサー パラメータを定義する方法と、ポリシー マップ内の複数のクラスにそのポリサーを適用する方法を示します。

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 8000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

設定を確認するには、**show mls qos aggregate-policer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos aggregate-policer	ポリシー マップ内の複数のクラスが共有できるポリサー パラメータを定義します。
show mls qos aggregate-policer	QoS (Quality of Service) 集約ポリサー設定を表示します。

policy-map

複数の物理ポートに適用できるポリシー マップを作成または変更し、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、**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*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

policy-map-name ポリシー マップ名です。

デフォルト

ポリシー マップは定義されません。

デフォルトの動作は、パケットが IP パケットの場合には Differentiated Service Code Point (DSCP) を 0 に設定し、パケットがタグ付きの場合にはサービス クラス (CoS) を 0 に設定します。ポリシー マップは実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

policy-map コマンドを入力すると、ポリシーマップ 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** : 指定されたクラス マップの分類一致条件を定義します。詳細については、[P.2-57](#) の「class」を参照してください。
- **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** : すでに定義済みのポリシー マップを削除します。
- **rename** : 現在のポリシー マップの名前を変更します。

グローバル コンフィギュレーション モードに戻る場合は、**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。クラスの一致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、入力ポートごとに 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。

例

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マッチングを行い、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。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

次の例では、ポリシー マップ *polycymap2* に複数のクラスを設定する方法を示します。

```
Switch(config)# policy-map polycymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp 0 (no policer)
Switch(config-pmap-c)# exit
```

次の例では、*polycymap2* を削除する方法を示します。

```
Switch(config)# no policy-map polycymap2
```

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。

関連コマンド

コマンド	説明
class	指定のクラスマップ名のトラフィック分類の一致基準を定義します (police 、 set 、および trust 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)。
class-map	名前を指定したクラスとパケットとの比較に使用されるクラス マップを作成します。
service-policy	ポートにポリシー マップを適用します。
show policy-map	QoS ポリシー マップを表示します。

port-channel load-balance

EtherChannel のポート間で負荷分散方式を設定するには、**port-channel load-balance** 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。

```
port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}
```

```
no port-channel load-balance
```

シンタックスの説明

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散。
dst-mac	宛先ホストの MAC (メディア アクセス制御) アドレスに基づいた負荷分散。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。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいた負荷分散。
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。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散。
src-mac	送信元 MAC アドレスに基づいた負荷分散。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。

デフォルト

デフォルトは、**src-mac** です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

これらの転送方式をどのような場合に使用するかについては、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。

例

次の例では、負荷分散方式を **dst-mac** に設定する方法を示します。

```
Switch(config)# port-channel load-balance dst-mac
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
interface port-channel	ポート チャンネルへのアクセスや、ポート チャンネルの作成を行います。
show etherchannel	チャンネルの EtherChannel 情報を表示します。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

power inline

Power over Ethernet (PoE) ポート上で電力管理モードを設定するには、**power inline** 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。

```
power inline {auto [max max-wattage] | never | police [action log] | static [max max-wattage]}
```

```
no power inline {auto | never | police | static}
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

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。
max max-wattage	(任意) ポート上で許可される電力を制限します。指定できる範囲は 4000 ~ 15400 ミリワットです。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。
police [action log]	リアルタイムの消費電力のポリシングをイネーブルにします。これらのキーワードの詳細については、 power inline police コマンドを参照してください。
static	受電装置の検出をイネーブルにします。スイッチが受電装置を検出する前に、ポートへの電力を事前に割り当てます (確保します)。

デフォルト

デフォルトの設定は **auto** (イネーブル) です。
最大ワット数は、15400 ミリワットです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。
12.2(46)SE	police [action log] キーワードが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応ポートのみ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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# power inline auto
                        ^
% Invalid input detected at '^' marker.
```


max max-wattage オプションを使用して、受電装置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、受電装置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 パワー バジレットに送られます。



(注)

power inline max max-wattage コマンドが 15.4 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。

スイッチが受電装置への電力供給を拒否する場合（受電装置が 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** ユーザ 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 max max-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 クラスまたは受電装置からの 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されているので、最大ワット数以下の電力を使用する受電装置は、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、受電装置の 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装置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、受電装置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に割り当てることができないと（たとえば、パワー バジレット全体が別の自動ポートまたはスタティック ポートにすでに割り当てられているため）、**Command rejected: power inline static: pwr not available** というメッセージが表示されます。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、受電装置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あと、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場合、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装置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。ポートで不正なリンクアップが生じ、**errdisable** ステートになる可能性があります。

例

次の例では、受電装置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。

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# power inline auto
```

次の例では、Class 1 または Class 2 の受電装置を受け入れるように PoE ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# power inline auto max 7000
```

power inline

次の例では、受電装置の検出をディセーブルにし、PoE ポートへの電力供給を停止する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# power inline never
```

設定を確認するには、**show power inline** ユーザ EXEC コマンドを入力します。

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのログギングをイネーブルにします。
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power inline consumption

各受電装置が使用するワット数を指定して、デバイスの IEEE 分類に指定された電力量を無効にするには、**power inline consumption** グローバルまたはインターフェイス コンフィギュレーション コマンドを使用します。デフォルトの電力設定に戻すには、このコマンドの **no** 形式を使用します。

power inline consumption default *wattage*

no power inline consumption default



(注) **default** キーワードは、グローバル コンフィギュレーション コマンドだけに表示されます。



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

wattage スイッチがポート用に確保する電力を指定します。指定できる範囲は 4000 ~ 15400 ミリワットです。

デフォルト

Power over Ethernet (PoE) ポートのデフォルトの電力は 15400 ミリワットです。

コマンドモード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

シスコの受電装置が PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol (CDP) を使用して実際に装置が消費する電力量を決定して、それに応じてパワー バジレットを調整します。この機能は、IEEE サードパーティの受電装置には適用されません。この装置の場合、スイッチが電力要求を許可したときに、受電装置の IEEE 分類に応じてパワー バジレットを調整します。受電装置が Class 0 (クラス ステータスは不明) または Class 3 である場合、実際に必要な電力量に関係なく、スイッチはポート用に 15400 ミリワットの電力を確保します。受電装置が実際の電力消費量よりも高いクラスであるか、または電力分類 (デフォルトで Class 0) をサポートしない場合、スイッチは IEEE クラス情報を使用してグローバル パワー バジレットを追跡するので、少しの装置にしか電力を供給しません。

power inline consumption *wattage* コンフィギュレーション コマンドを使用することで、IEEE 分類で指定されたデフォルトの電力要件を無効にできます。IEEE 分類で指定された電力と実際に装置が必要とする電力の差は、追加の装置が使用するためグローバル パワー バジレットに入れられます。したがって、スイッチのパワー バジレットを拡張してもっと効率的に使用できます。

たとえば、スイッチが各 PoE ポートで 15400 ミリワットの電力を確保した場合、Class0 の受電装置を 24 台だけしか接続できません。Class0 の装置の電力要件が実際には 5000 ミリワットである場合、消費ワット数を 5000 ミリワットに設定すると、最大 48 台の装置を接続できます。24 ポートまたは 48 ポートスイッチで利用できる PoE 総出力電力は 370,000 ミリワットです。



注意

慎重にスイッチのパワー バジェットを計画し、電源装置がオーバーサブスクライブ状態にならないようにしてください。

power inline consumption default wattage または **no power inline consumption default** グローバル コンフィギュレーション コマンド、あるいは **power inline consumption wattage** または **no power inline consumption** 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場合、次の注意メッセージが表示されます。

```
%CAUTION: Interface interface-id: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```



(注)

手動でパワー バジェットを設定する場合、スイッチと受電装置の間のケーブルでの電力消失を考慮する必要があります。

IEEE 電力分類の詳細については、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 ガイドの「Configuring Interface Characteristics」の章を参照してください。

このコマンドは、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スイッチ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。

例

次の例では、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、各 PoE ポートに 5000 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# power inline consumption default 5000
%CAUTION: Interface Gi0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

次の例では、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 PoE ポートに接続された受電装置に 12000 ミリワットの電力を確保するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# power inline consumption 12000
%CAUTION: Interface Gi0/2: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.Refer to documentation.
```

設定を確認するには、**show power inline consumption** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
power inline	PoE ポート上で電力管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

power inline police

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、**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。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 log]

no power inline police

シンタックスの説明

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、スイッチは接続された装置に電力を供給しながら Syslog メッセージを生成します。 action log キーワードを入力しない場合に、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すると、スイッチはポートへの電力供給をオフにします (デフォルトのアクション)。
-------------------	---

デフォルト

受電装置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。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(46)SE	このコマンドが追加されました。

使用上のガイドライン

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スイッチ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。

power inline police [action log] コマンドは、PoE ポートを備えたスイッチのみでサポートされていません。

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、受電装置が割り当てられた最大電力より多くの量を消費すると、スイッチが対処します。

PoE がイネーブルである場合、スイッチは受電装置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、スイッチは **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、次の順のいずれかの方式で PoE ポートのカットオフ電力が判別されます。

1. **power inline consumption default wattage** グローバル コンフィギュレーション コマンドまたは **power inline consumption wattage** インターフェイス コンフィギュレーション コマンドを入力する場合、スイッチがポート用に確保するユーザ定義の電力レベル
2. **power inline auto max max-wattage** 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 コマンドを入力する場合、ポートで許可される電力を制限するユーザ定義の電力レベル

3. CDP パワー ネゴシエーションまたは装置の IEEE 分類を使用してスイッチが設定した装置の消費電力
4. スイッチが設定したデフォルトの消費電力（デフォルト値は 15.4 W）

power inline consumption default wattage グローバル コンフィギュレーション コマンド、**power inline consumption 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 [auto | static max] max-wattage** コマンドを入力して、カットオフ電力値を手動で設定するには、上記リストの 1 番めおよび 2 番めの方式を使用します。手動でカットオフ電力値を設定していない場合、スイッチが CDP パワー ネゴシエーションまたは装置の IEEE 分類を使用して、カットオフ電力値を自動的に決定します。これが上記リストの 3 番めの方式となります。スイッチがこれらのいずれの方式を使用しても値を決定できない場合、15.4 W というデフォルト値を使用します（上記リストの 4 番めの方式）。



(注)

カットオフ電力値、スイッチが使用する電力消費値、および接続装置の実際の電力消費値については、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 Interface Characteristics」の章の「Power Monitoring and Power Policing」を参照してください。

パワー ポリシングがイネーブルである場合、スイッチ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、スイッチはポートへの電力供給をオフにするか、または装置に電力を供給しながら Syslog メッセージを生成して LED（オレンジに点滅）を更新します。

- ポートへの電力供給をオフにして、ポートを **errdisable** ステートとするようスイッチを設定するには、**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スイッチを設定するには、**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 **errdisable** ステートに移行、になります。PoE ポートを **errdisable** 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 **errdisable** 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 **errdisable** 原因の回復タイマーをイネーブルにします。



注意

ポリシングがディセーブルである場合、受電装置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、スイッチに悪影響を与える場合があります。

例

次の例では、電力消費のポリシングをイネーブルにして、スイッチの PoE ポートで Syslog メッセージを生成するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# power inline police action log
```

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。

関連コマンド

コマンド	説明
<code>errdisable detect cause inline-power</code>	PoE 原因に対する <code>errdisable</code> 検出をイネーブルにします。
<code>errdisable recovery cause inline-power</code>	PoE 回復メカニズム変数を設定します。
<code>power inline</code>	PoE ポート上で電力管理モードを設定します。
<code>power inline consumption</code>	IEEE 分類によって受電装置に指定された電力量を上書きします。
<code>show power inline police</code>	リアルタイムの電力消費についてのパワー ポリシング情報を表示します。

priority-queue

ポート上で出力緊急キューをイネーブルにするには、**priority-queue** 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。

priority-queue out

no priority-queue out

シンタックスの説明

out 出力緊急キューをイネーブルにします。

デフォルト

出力緊急キューは、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

priority-queue out コマンドを設定する場合、シェイプド ラウンド ロビン (SRR) に参加するキューが 1 つ少ないため、SRR の重み比が影響を受けます。これは、**srr-queue bandwidth shape** 内の *weight1* または **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドが無視されることを意味します (比率計算に使用されません)。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して **shaped** モードは **shared** モードを無効にし、SRR はこのキューに **shaped** モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR はキューに対して **shared** モードでサービスを提供します。

例

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```


次の例では、SRR のシェーピングおよび共有された重みが設定されたあと、出力緊急キューをディセーブルにする方法を示します。シェーピング モードは、共有モードを無効にします。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

show mls qos interface interface-id queueing または **show running-config** 特権 EXEC コマンドを入力すれば、設定を確認することができます。

関連コマンド

コマンド	説明
show mls qos interface queueing	(任意) キューイング方法 (SRR、プライオリティ キューイング)、キューに相応する重み、およびサービス クラス (CoS) から出力キューへのマップを表示します。
srr-queue bandwidth shape	シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅のシェーピングをイネーブルにします。
srr-queue bandwidth share	共有ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

queue-set

ポートをキューセットにマッピングするには、**queue-set** 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。

queue-set *qset-id*

no queue-set *qset-id*



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

qset-id キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ~ 2 です。

デフォルト

キューセット ID は 1 です。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface [interface-id] buffers** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。
show mls qos interface buffers	QoS (Quality of Service) 情報を表示します。

radius-server dead-criteria

RADIUS サーバが使用不可またはデッド状態であると判断する条件を設定するには、**radius-server dead-criteria** 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。

radius-server dead-criteria [*time seconds* [*tries number*] | *tries number*]

no radius-server dead-criteria [*time seconds* [*tries number*] | *tries number*]

シンタックスの説明

time seconds	(任意) RADIUS サーバからの有効な応答をスイッチが取得するのに必要としない時間 (秒) を設定します。指定できる範囲は 1 ~ 120 秒です。
tries number	(任意) サーバが使用不可と見なされる前に RADIUS サーバから有効な応答をスイッチが取得するのに必要としない回数を指定します。指定できる範囲は 1 ~ 100 です。

デフォルト

スイッチは、10 ~ 60 秒の *seconds* 値を動的に決定します。

スイッチは、10 ~ 100 の *tries* 値を動的に決定します。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

次の *seconds* および *number* パラメータを設定することを推奨します。

- IEEE 802.1x 認証が期限切れになる前に RADIUS サーバへの応答を待機する時間 (秒) を指定するには、**radius-server timeout seconds** 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。スイッチは、10 ~ 60 秒のデフォルトの *seconds* 値を動的に決定します。
- RADIUS サーバが使用不能と見なされる前に RADIUS サーバへの送信を試行する時間 (秒) を指定するには、**radius-server retransmit retries** 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。スイッチは、10 ~ 100 のデフォルトの *tries* 値を動的に決定します。
- *seconds* パラメータは、IEEE 802.1x 認証が期限切れになる前に再送信を試行する秒数以下か、または同じです。
- *tries* パラメータは、再送信試行回数と同じである必要があります。

例

次の例では、RADIUS サーバが使用不可と見なされた場合に決定する条件として、**time** に 60 を設定し、**tries** の回数に 10 を設定する方法を示します。

```
Switch(config)# radius-server dead-criteria time 60 tries 10
```

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。

関連コマンド	コマンド	説明
	dot1x critical (グローバル コンフィギュレーション)	アクセス不能な認証バイパス機能のパラメータを設定します。
	dot1x critical (インターフェイス コンフィギュレーション)	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定します。
	radius-server retransmit <i>retries</i>	RADIUS サーバが使用不可と見なされる前にスイッチが RADIUS サーバに送信を試行する回数を指定します。構文情報については、「Cisco IOS Security Command Reference, Release 12.2」>「Server Security Protocols」>「RADIUS Commands」を選択します。
	radius-server timeout <i>seconds</i>	IEEE 802.1x 認証が期限切れになる前にスイッチが RADIUS サーバへの応答を待機する時間 (秒) を指定します。構文情報については、「Cisco IOS Security Command Reference, Release 12.2」>「Server Security Protocols」>「RADIUS Commands」を選択します。
	show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

radius-server host

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、**radius-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。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 host *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name*] [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**] [**key** *string*]

no radius-server host *ip-address*

シンタックスの説明

<i>ip-address</i>	RADIUS サーバの IP アドレスを指定します。
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。
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。
test username <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。
idle-time <i>time</i>	(任意) スイッチがテストパケットをサーバに送信したあとの間隔 (分) を設定します。指定できる範囲は 1 ~ 35791 分です。
ignore-acct-port	(任意) RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。
ignore-auth-port	(任意) RADIUS サーバ認証ポートのテストをディセーブルにします。
key <i>string</i>	(任意) スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証鍵および暗号鍵を指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。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。先頭のスペースは無視されますが、key 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 の一部でないかぎり、key を引用符で囲まないでください。

デフォルト

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。

アイドル時間は 60 分 (1 時間) です。

自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。

認証鍵および暗号鍵 (*string*) は設定されていません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

RADIUS アカウンティング 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、**test username name** キーワードを使用します。

radius-server host ip-address key string または **radius-server key {0 string | 7 string | string}** 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認証鍵および暗号鍵を設定できます。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。

例

次の例では、アカウンティング サーバの UDP ポートを 1500、認証サーバの UDP ポートを 1510 に設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.1 acct-port 1500 auth-port 1510
```

次の例では、アカウンティング サーバおよび認証サーバの UDP ポートを設定し、RADIUS サーバステータスの自動テストをイネーブルにし、使用されるユーザ名を指定し、キー スtring を設定する例を示します。

```
Switch(config)# radius-server host 1.1.1.2 acct-port 800 auth-port 900 test username  
aaafail idle-time 75 key abc123
```

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。

関連コマンド

コマンド	説明
dot1x critical (グローバル コンフィギュレーション)	アクセス不能な認証バイパス機能のパラメータを設定します。
dot1x critical (インターフェイス コンフィギュレーション)	アクセス不能な認証バイパス機能をインターフェイス上でイネーブルにし、ポートが critical-authentication ステートに置かれた場合にスイッチがクリティカルなポートに割り当てるアクセス VLAN を設定します。
radius-server key {0 string 7 string string}	ルータおよび RADIUS デモン間のすべての RADIUS コミュニケーションの認証鍵および暗号鍵を指定します。構文情報については、「Cisco IOS Security Command Reference, Release 12.2」>「Server Security Protocols」>「RADIUS Commands」を選択します。
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

rcommand

Telnet セッションを開始し、クラスタ コマンド スイッチからクラスタ メンバー スイッチのコマンドを実行するには、クラスタ コマンド スイッチで **rcommand** ユーザ EXEC コマンドを使用します。セッションを終了するには、**exit** コマンドを入力します。

```
rcommand {n | commander | mac-address hw-addr}
```

シンタックスの説明

<i>n</i>	クラスタ メンバーを識別する番号を提供します。指定できる範囲は 0 ~ 15 です。
commander	クラスタ メンバー スイッチからクラスタ コマンド スイッチへアクセスできるようにします。
mac-address hw-addr	クラスタ メンバー スイッチの MAC (メディア アクセス制御) アドレス

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でのみ利用できます。

スイッチがクラスタ コマンド スイッチで、クラスタ メンバー スイッチ *n* が存在していない場合、エラー メッセージが表示されます。スイッチ番号を得るには、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。

このコマンドを使用してクラスタ コマンド スイッチ プロンプトからクラスタ メンバー スイッチにアクセスしたり、メンバー スイッチ プロンプトからクラスタ コマンド スイッチにアクセスしたりすることができます。

Catalyst 2900 XL、Catalyst 3500 XL、Catalyst 2950、Catalyst 2960、Catalyst 2970、Catalyst 3550、Catalyst 3560、および Catalyst 3750 スイッチの場合、Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバー スイッチ CLI (コマンドライン インターフェイス) にアクセスします。たとえば、このコマンドをクラスタ コマンド スイッチからユーザ レベルで入力した場合、メンバー スイッチはユーザ レベルでアクセスされます。このコマンドをクラスタ コマンド スイッチからイネーブル レベルで使用した場合、コマンドはイネーブル レベルでリモート デバイスにアクセスします。権限レベルよりも低い中間イネーブル レベルを使用した場合、クラスタ メンバー スイッチはユーザ レベルとなります。

Standard Edition ソフトウェアが稼動している Catalyst 1900 スイッチと Catalyst 2820 スイッチでは、クラスタ コマンド スイッチが権限レベル 15 の場合、Telnet セッションはメニュー コンソール (メニュー方式 インターフェイス) にアクセスします。クラスタ コマンド スイッチが権限レベル 1 の場合

は、パスワードの入力を要求するプロンプトが表示され、入力後にメニュー コンソールにアクセスできます。クラスタ コマンド スイッチの権限レベルは、Standard Edition ソフトウェアが稼動しているクラスタ メンバー スイッチに次のようにマッピングします。

- クラスタ コマンド スイッチの権限レベルが 1 ～ 14 である場合、クラスタ メンバー スイッチへのアクセスは権限レベル 1 で行われます。
- クラスタ コマンド スイッチの権限レベルが 15 である場合、クラスタ メンバー スイッチへのアクセスは権限レベル 15 で行われます。

Catalyst 1900 および Catalyst 2820 の CLI が利用できるのは、スイッチで Enterprise Edition ソフトウェアが稼動している場合に限られます。

クラスタ コマンド スイッチの vty ラインにアクセス クラス コンフィギュレーションがある場合、このコマンドは機能しません。

クラスタ メンバー スイッチはクラスタ コマンド スイッチのパスワードを継承するため、クラスタ メンバー スイッチがクラスタに加入してもパスワードを要求するプロンプトは表示されません。

例

次の例では、メンバー 3 でセッションを開始する方法を示します。**exit** コマンドを入力するか、またはセッションを閉じるまで、このコマンドに続くすべてのコマンドがメンバー 3 に向けられます。

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

関連コマンド

コマンド	説明
show cluster members	クラスタ メンバーに関する情報を表示します。

remote-span

VLAN をリモート スイッチド ポート アナライザ (RSPAN) VLAN として設定するには、**remote-span** VLAN コンフィギュレーション コマンドを使用します。RSPAN 指定を VLAN から削除するには、このコマンドの **no** 形式を使用します。

remote-span

no remote-span



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

RSPAN VLAN は定義されません。

コマンド モード

VLAN コンフィギュレーション (config-VLAN)

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

RSPAN VLAN を設定できるのは config-VLAN モードの場合だけです (このモードは、**vlan** グローバル コンフィギュレーション コマンドで開始します)。**vlan database** 特権 EXEC コマンドを使用して開始された VLAN コンフィギュレーション モードでは設定できません。

VLAN トランッキング プロトコル (VTP) がイネーブルであり、VLAN ID が 1005 未満の場合は、RSPAN 機能が VTP で伝達されます。RSPAN VLAN ID が拡張範囲内にある場合は、手動で中間スイッチ (送信元スイッチと宛先 X イッチ間の RSPAN VLAN にあるスイッチ) を設定する必要があります。

RSPAN **remote-span** コマンドを設定する前に、**vlan** (グローバル コンフィギュレーション) コマンドで VLAN を作成してください。

RSPAN VLAN には、次の特性があります。

- MAC アドレス ラーニングは実行されません。
- トランク ポートでは RSPAN VLAN トラフィックのみが流れます。
- Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) は RSPAN VLAN 内では稼働できますが、RSPAN 宛先ポートでは稼働しません。

既存の VLAN が RSPAN VLAN として設定されている場合は、その VLAN が最初に削除され、RSPAN VLAN として再作成されます。アクセス ポートは、RSPAN 機能がディセーブルになるまでは非アクティブです。

例

次の例では、RSPAN VLAN として VLAN を設定する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

次の例では、VLAN から RSPAN 機能を削除する方法を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

show vlan remote-span ユーザ EXEC コマンドを入力すると、設定を確認することができます。

関連コマンド

コマンド	説明
monitor session	ポートでスイッチドポートアナライザ (SPAN) および RSPAN モニタリングをイネーブルにし、ポートを送信元ポートまたは宛先ポートとして設定します。
vlan (グローバル コンフィギュレーション)	VLAN 1 ~ 4094 を設定できる config-vlan モードに変更します。

renew ip dhcp snooping database

DHCP スヌーピング バインディング データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

```
renew ip dhcp snooping database [{flash:/filename | ftp://user:password@host/filename |
nvrRam:/filename | rcp://user@host/filename | tftp://host/filename}] [validation none]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

flash:/filename	(任意) データベース エージェントまたはバインディング ファイルがフラッシュ メモリにあることを指定します。
ftp://user:password@host/filename	(任意) データベース エージェントまたはバインディング ファイルが FTP (ファイル転送プロトコル) サーバにあることを指定します。
nvrAm:/filename	(任意) データベース エージェントまたはバインディング ファイルが NVRAM にあることを指定します。
rcp://user@host/file name	(任意) データベース エージェントまたはバインディング ファイルが Remote Control Protocol (RCP) サーバにあることを指定します。
tftp://host/filename	(任意) データベース エージェントまたはバインディング ファイルが TFTP (簡易ファイル転送プロトコル) サーバにあることを指定します。
validation none	(任意) URL によって指定されたバインディング ファイルのエントリに対して、Cyclic Redundancy Check (CRC; 巡回冗長検査) を検証しないようにスイッチに指定します。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

URL を指定しない場合は、スイッチは設定された URL からファイルを読み込もうとします。

例

次の例では、ファイル内の CRC 値のチェックを省略して、DHCP スヌーピング バインディング データベースを更新する方法を示します。

```
Switch# renew ip dhcp snooping database validation none
```

設定を確認するには、**show ip dhcp snooping database** 特権 EXEC コマンドを入力します。

■ renew ip dhcp snooping database

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
show ip dhcp snooping database	DHCP スヌーピング データベース エージェントのステータスを表示します。

reserved-only

Dynamic Host Configuration Protocol (DHCP) アドレス プール内で予約済のアドレスだけを割り当てるには、**reserved-only** DHCP プール コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

reserved-only

no reserved-only

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトでは、プールアドレスを制限しない設定になっています。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン **reserved-only** コマンドを入力すると、DHCP プールからの割り当てが予約済のアドレスに制限されます。ネットワークの一部となっている未予約のアドレスやプールの範囲内にある未予約のアドレスが該当するクライアントに割り当てられなくなります。また、それ以外のクライアントには、プールからアドレスが提供されません。

ユーザはこのコマンドを使用して、DHCP プールを装備した 1 組のスイッチが共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視するように設定できます。

DHCP プール コンフィギュレーション モードにアクセスするには、**ip dhcp pool name** グローバル コンフィギュレーション コマンドを入力します。

例 次の例では、予約済のアドレスだけを割り当てるように DHCP プールを設定する方法を示します。

```
Switch# config t
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

設定を確認するには、**show ip dhcp pool** 特権 EXEC コマンドを入力します。

■ reserved-only

関連コマンド

コマンド	説明
<code>show ip dhcp pool</code>	DHCP アドレス プールを表示します。

rmon collection stats

イーサネット グループの統計（ブロードキャスト パケットおよびマルチキャスト パケットに関する使用率の統計と巡回冗長検査 [CRC] 整合性エラーおよび衝突に関するエラー統計を含む）を収集するには、**rmon collection stats** 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。

rmon collection stats index [owner name]

no rmon collection stats index [owner name]

シンタックスの説明	
<i>index</i>	Remote Network Monitoring (RMON) 収集制御インデックス。指定できる範囲は 1 ~ 65535 です。
<i>owner name</i>	(任意) RMON 収集の所有者。

デフォルト RMON 統計情報収集はディセーブルです。

コマンドモード インターフェイス コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン RMON 統計情報収集コマンドはハードウェア カウンタに基づいています。

例 次の例では、所有者 *root* の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```

設定を確認するには、**show rmon statistics** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show rmon statistics	RMON 統計情報を表示します。 構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「System Management Commands」 > 「RMON Commands」を選択してください。

sdm prefer

Switch Database Management (SDM) リソース割り当てで使用されるテンプレートを設定するには、**sdm prefer** 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。テンプレートを使用して、システム リソースがアプリケーションで使用されている機能をフルにサポートできるように割り当てたり、IPv6 フォワーディングをサポートするためにデュアル IPv4 および IPv6 テンプレートを選択したりすることができます (スイッチで LAN Base イメージが実行されている場合にのみサポートされます)。デフォルトのテンプレートに戻すには、このコマンドの **no** 形式を使用します。

```
sdm prefer {default | dual-ipv4-and-ipv6 default | qos}
```

```
no sdm prefer
```

シンタックスの説明

default	すべての機能に対してバランスを取ります。
dual-ipv4-and-ipv6 default	(注) デュアル スタック環境でのスイッチの使用を可能にします (IPv4 および IPv6 両方のフォワーディングをサポート)。このテンプレートを設定して、IPv6 MLD スヌーピング機能または IPv6 ホスト機能をイネーブルにする必要があります。
qos	最大限のシステム リソースを QoS (Quality of Service) アクセス コントロール エントリ (ACE) に割り当てます。

デフォルト

default テンプレートはすべての機能を均等に動作させます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(40)SE	dual-ipv4-and-ipv6 default キーワードが追加されました。

使用上のガイドライン

この設定を有効にするには、スイッチをリロードする必要があります。

reload 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** により、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

スイッチをデフォルト デスクトップ テンプレートに設定するには、**no sdm prefer** コマンドを使用します。

スイッチで IPv6 MLD スヌーピングまたはホスト機能を含む IPv6 ルーティングをイネーブルにしない場合は、IPv4/IPv6 テンプレートを使用しないでください。**sdm prefer ipv4-and-ipv6 default** グローバル コンフィギュレーション コマンドを入力すると、リソースを IPv4 と IPv6 に振り分けて、IPv4 フォワーディングに割り当てられたリソースを制限します。

表 2-17 に、各テンプレートでサポートされているリソースの概算を示します。

表 2-17 各テンプレートに割り当てられた機能のリソースの概算

リソース	デフォルト	QoS	デュアル
ユニキャスト MAC アドレス	8 K	8 K	8 K
IPv4 IGMP グループ	256	256	256
IPv4 ユニキャスト ルート	0	0	0
IPv6 マルチキャスト グループ	0	0	0
直接接続された IPv6 アドレス	0	0	0
間接 IPv6 ユニキャスト ルート	0	0	0
IPv4 ポリシー ベース ルーティング ACE	0	0	0
IPv4 MAC QoS ACE	128	384	0
IPv4 MAC セキュリティ ACE	384	128	256
IPv6 ポリシー ベース ルーティング ACE	0	0	0
IPv4 MAC QoS ACE	0	0	0
IPv4 MAC セキュリティ ACE	0	0	0

例

次の例では、QoS テンプレートの使用方法を示します。

```
Switch(config)# sdm prefer qos
Switch(config)# exit
Switch# reload
```

次の例では、スイッチ上でデフォルトのデュアル IPv4/IPv6 テンプレートを設定する方法を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
```

設定を確認するには、**show sdm prefer** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show sdm prefer	現在使用されている SDM テンプレート、または機能ごとのリソース割り当ての概算による使用可能なテンプレートを表示します。

service password-recovery

パスワード回復メカニズムをイネーブル（デフォルト）にするには、**service password-recovery** 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。このメカニズムでは、スイッチに物理的にアクセスするエンドユーザは、スイッチの電源投入時に **Mode** ボタンを押して起動プロセスを中断し、新しいパスワードを割り当てることができます。パスワード回復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。パスワード回復メカニズムがディセーブルになると、ユーザがシステムをデフォルト設定に戻すことに同意した場合にのみブート プロセスを中断できます。

service password-recovery

no service password-recovery

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

パスワード回復メカニズムはイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

システム管理者は **no service password-recovery** コマンドを使用して、パスワード回復機能の一部をディセーブルにできます。これによりエンドユーザは、システムをデフォルト設定に戻すことに同意した場合のみ、パスワードをリセットすることが可能です。

パスワード回復手順を実行する場合、スイッチに物理的にアクセスするユーザは、スイッチの電源投入時とポート 1X の上にある LED が消灯してから 1 ～ 2 秒後に **Mode** ボタンを押します。ボタンを放すと、システムは初期化を続けます。

パスワード回復メカニズムがディセーブルの場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```



(注)

ユーザがシステムをデフォルト設定にリセットしない場合、**Mode** ボタンを押さない場合と同じように通常の起動プロセスが続行します。システムをデフォルト値に戻すように設定すると、フラッシュメモリ内のコンフィギュレーション ファイルが削除され、VLAN データベース ファイル *flash:vlan.dat* が存在する場合は、そのファイルも削除されます。**no service password-recovery** コマンドを使用してパスワードへのエンドユーザのアクセスを制御する場合は、エンドユーザがパスワード回復手順を実行してシステムをデフォルト値に戻す状況を考慮し、スイッチとは別の場所に **config** ファイルのコ

ピーを保存しておくことを推奨します。スイッチ上に `config` ファイルのバックアップを保存しないでください。

スイッチが VTP 透過モードで動作している場合、`vlan.dat` ファイルもスイッチとは別の場所にコピーを保存しておくことを推奨します。

パスワードの回復がイネーブルかどうか確認するには、**show version** 特権 EXEC コマンドを入力します。

例

次の例では、スイッチ上でパスワード回復をディセーブルにする方法を示します。ユーザはデフォルト設定に戻すことに同意が得られた場合のみパスワードをリセットできます。

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

関連コマンド

コマンド	説明
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

service-policy

policy-map コマンドで定義されたポリシー マップを物理ポートの入力に適用するには、**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 policy-map-name

no service-policy input policy-map-name



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

input policy-map-name 物理ポートの入力に、指定したポリシー マップを適用します。



(注) **history** キーワードは、コマンドラインのヘルプ スtringには表示されますが、サポートされていません。このキーワードが収集した統計情報は無視します。**output** キーワードもサポートされていません。

デフォルト

ポートにポリシー マップは適用されていません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ポリシー マップは、物理ポート上に設定できます。

物理ポート上の着信トラフィックにポリシー マップを適用できます。

ポート信頼状態を使用した分類（たとえば、**mls qos trust [cos | dscp | ip-precedence]**）とポリシー マップ（たとえば、**service-policy input policy-map-name**）は同時に指定できません。最後に行われた設定により、前の設定が上書きされます。

例

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。

```
Switch(config)# interface gigabitethernet0/1
Switch(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。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy input plcmap2
```

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。

関連コマンド

コマンド	説明
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー マップを作成または変更します。
show policy-map	QoS ポリシー マップを表示します。
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

set

パケットの Differentiated Service Code Point (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、**set** 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。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 {dscp new-dscp | [ip] precedence new-precedence}
```

```
no set {dscp new-dscp | [ip] precedence new-precedence}
```

シンタックスの説明

dscp new-dscp	分類されたトラフィックに割り当てられる新しい DSCP 値です。指定できる範囲は 0 ~ 63 です。よく使用する値の場合は、ニーモニック名を入力することもできます。
[ip] precedence new-precedence	分類されたトラフィックに割り当てられる新しい IP precedence 値です。指定できる範囲は 0 ~ 7 です。よく使用する値の場合は、ニーモニック名を入力することもできます。

デフォルト

トラフィックの分類は定義されていません。

コマンドモード

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	ip キーワードは任意です。

使用上のガイドライン

set ip dscp ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、スイッチによってこのコマンドがスイッチ コンフィギュレーションの **set dscp** に変更されます。**set ip dscp** ポリシー マップ クラス コンフィギュレーション コマンドを入力すると、スイッチ コンフィギュレーションではこの設定は **set dscp** として表示されます。

set ip precedence または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドのいずれかを使用できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。

同じポリシーマップ内では、**set** コマンドと **trust** ポリシーマップ クラス コンフィギュレーション コマンドを同時に指定できません。

set dscp new-dscp コマンドまたは **set ip precedence new-precedence** コマンドについては、一般的な値にニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力できます。これは **set dscp 10** コマンドの入力と同じです。**set ip precedence critical** コマンドを入力できます。これは **set ip precedence 5** コマンドの入力と同じです。サポートされているニーモニックのリストについては、**set dscp ?** または **set ip precedence ?** コマンドを入力して、コマンドライン ヘルプ スtring 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。

例 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 を割り当てます。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(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。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件 (police 、 set 、および trust ポリシーマップ クラス コンフィギュレーション コマンドによる) を定義します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに適用することによってサービスポリシーを指定できるポリシーマップを作成または変更します。
show policy-map	QoS ポリシー マップを表示します。
trust	class ポリシーマップ コンフィギュレーション コマンドまたは class-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分類されたトラフィックの信頼状態を定義します。

setup

スイッチを初期設定に設定するには、**setup** 特権 EXEC コマンドを使用します。

setup

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

setup コマンドを使用する場合、次の情報が必要になります。

- IP アドレスおよびネットワーク マスク
- 使用環境に対するパスワードの方針
- スイッチがクラスタ コマンド スイッチおよびクラスタ名として使用されるかどうか

setup コマンドを入力すると、**System Configuration Dialog** という対話形式のダイアログが表示されます。コンフィギュレーション プロセスが開始され、情報を求めるプロンプトが表示されます。各プロンプトの隣のカッコに表示される値は、**setup** コマンド機能または **configure** 特権 EXEC コマンドを使用して設定された最後のデフォルト値です。

各プロンプトでヘルプ テキストが提供されます。ヘルプ テキストにアクセスするには、プロンプトで疑問符 (?) のキーを入力します。

変更を中断し、**System Configuration Dialog** を最後まで実行せずに特権 EXEC プロンプトに戻るには、**Ctrl-C** を押します。

変更が完了した場合、セットアッププログラムにより、セットアップセッション中に作成されたコンフィギュレーション コマンド スクリプトが表示されます。設定を NVRAM (不揮発性 RAM) に保存するか、あるいは設定を保存せずにセットアッププログラムまたはコマンドライン プロンプトに戻ることができます。

例

次の例では、**setup** コマンドの出力を示します。

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.
```



```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
Enter host name [Switch]:host-name
```

```
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: enable-secret-password
```

```
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: enable-password
```

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: terminal-password
```

```
Configure SNMP Network Management? [no]: yes
Community string [public]:
```

```
Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	172.20.135.202	YES	NVRAM	up	up

GigabitEthernet0/1	unassigned	YES	unset	up	up
--------------------	------------	-----	-------	----	----

GigabitEthernet0/2	unassigned	YES	unset	up	down
--------------------	------------	-----	-------	----	------

<output truncated>

Port-channel1	unassigned	YES	unset	up	down
---------------	------------	-----	-------	----	------

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

```
Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: ip_address
Subnet mask for this interface [255.0.0.0]: subnet_mask
```

```
Would you like to enable as a cluster command switch? [yes/no]: yes
```

```
Enter cluster name: cluster-name
```

```
The following configuration command script was created:
```

```
hostname host-name
enable secret 5 $1$LiBw$0XclwyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!
```

```

cluster enable cluster-name
!
end
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:

```

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

setup express

Express Setup モードをイネーブルにするには、**setup express** 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。Express Setup モード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。

setup express

no setup express

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト Express Setup はイネーブルです。

コマンド モード グローバル コンフィギュレーション

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン 新しいスイッチ（未設定）上で Express Setup をイネーブルにする場合、Mode ボタンを 2 秒間押すことで Express Setup を開始できます。IP アドレス 10.0.0.1 を使用するとイーサネット ポート経由でスイッチにアクセスできます。そのあと、スイッチを Web ベースの Express Setup プログラム、または CLI（コマンドライン インターフェイス）ベースのセットアップ プログラムで設定できます。

設定したスイッチで Mode ボタンを 2 秒間押すと、Mode ボタンの上にある LED が点滅し始めます。Mode ボタンを 10 秒間押すと、スイッチの設定は削除され、スイッチが再起動します。その場合、スイッチは新規の状態になり、Web ベースの Express Setup または CLI ベースのセットアップ プログラムで、設定しなおすことができます。



(注) 設定の変更（CLI ベースのセットアップ プログラムの始めで **no** を入力することを含む）を行うとすぐに、Express Setup による設定を利用できなくなります。Mode ボタンを 10 秒間押し続けると、再度 Express Setup のみを稼動できます。これにより、設定は削除され、スイッチが再起動します。

スイッチ上で Express Setup がアクティブな場合に、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力すると、Express Setup は稼動しなくなります。スイッチの IP アドレス 10.0.0.1 は有効ではなくなり、この IP アドレスを使用している接続も終了します。

no setup express コマンドの主な目的は、Mode ボタンを 10 秒間押すことによってスイッチの設定が削除されるのを防ぐことです。

例 次の例では、Express Setup モードをイネーブルにする方法を示します。

```
Switch(config)# setup express
```

Mode ボタンを押すと、Express Setup モードがイネーブルであることを確認できます。

- 未設定のスイッチでは、Mode ボタンの上にある LED は 3 秒後にグリーンになります。
- 設定されたスイッチ上では、Mode の LED が 2 秒後に点滅し、10 秒後にグリーンになります。

**注意**

Mode ボタンを 10 秒間押し続けると、設定が削除され、スイッチが再起動します。

次の例では、Express Setup モードをディセーブルにする方法を示します。

```
Switch(config)# no setup express
```

Mode ボタンを押すと、Express Setup モードがディセーブルであることを確認できます。Express Setup モードがスイッチでイネーブルでない場合、モード LED はグリーンに点灯しない、またはグリーンに点滅し始めます。

関連コマンド

コマンド	説明
show setup express	Express Setup モードがアクティブかどうか表示します。

shell trigger

イベント トリガーを作成するには、**shell trigger** 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。イベント トリガーを削除する場合は、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*

シンタックスの説明

<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。

デフォルト

次のシステム定義のイベント トリガーが用意されています。

- CISCO_PHONE_EVENT
- CISCO_SWITCH_EVENT
- CISCO_ROUTER_EVENT
- CISCO_WIRELESS_AP_EVENT
- CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、**macro auto execute** グローバル コンフィギュレーション コマンドで使用されるユーザ定義のイベント トリガーを作成できます。

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、Cisco 属性と値 (AV) 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。

```
Switch# configure terminal
Switch(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event
Switch(config)# end
```

関連コマンド

コマンド	説明
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto execute	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設定します。
show shell	イベント トリガーとマクロに関する情報を表示します。

show access-lists

スイッチ上に設定されたアクセス コントロール リスト (ACL) を表示するには、**show access-lists** 特権 EXEC コマンドを使用します。

```
show access-lists [name | number | hardware counters | ipc] [| {begin | exclude | include}
expression]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>name</i>	(任意) ACL の名前です。
<i>number</i>	(任意) ACL の番号です。指定できる範囲は 1 ~ 2699 です。
hardware counters	(任意) スイッチングおよびルーティングされたパケットのグローバルハードウェア ACL 統計情報を表示します。
ipc	(任意) Interprocess Communication (IPC; プロセス間通信) プロトコルアクセス リスト コンフィギュレーションのダウンロード情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注) **rate-limit** 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ていますが、サポートされていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチは IP 標準および拡張アクセス リストのみをサポートします。したがって、1 ~ 199 と 1300 ~ 2699 のみが許可されます。

このコマンドでは、設定された MAC ACL も表示します。

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 次の例では、**show access-lists** コマンドの出力を示します。

```
Switch# show access-lists
Standard IP access list 1
  10 permit 1.1.1.1
  20 permit 2.2.2.2
  30 permit any
  40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
  10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
  10 permit 10.10.10.10
Extended IP access list 121
  10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
Extended IP access list CMP-NAT-ACL
  Dynamic Cluster-HSRP deny ip any any
  10 deny ip any host 19.19.11.11
  20 deny ip any host 10.11.12.13
  Dynamic Cluster-NAT permit ip any any
  10 permit ip host 10.99.100.128 any
  20 permit ip host 10.46.22.128 any
  30 permit ip host 10.45.101.64 any
  40 permit ip host 10.45.20.64 any
  50 permit ip host 10.213.43.128 any
  60 permit ip host 10.91.28.64 any
  70 permit ip host 10.99.75.128 any
  80 permit ip host 10.38.49.0 any
```

次の例では、**show access-lists hardware counters** コマンドの出力を示します。

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
  Drop: All frame count: 855
  Drop: All bytes count: 94143
  Drop And Log: All frame count: 0
  Drop And Log: All bytes count: 0
  Bridge Only: All frame count: 0
  Bridge Only: All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU: All frame count: 0
  Forwarding To CPU: All bytes count: 0
  Forwarded: All frame count: 2121
  Forwarded: All bytes count: 180762
  Forwarded And Log: All frame count: 0
  Forwarded And Log: All bytes count: 0

L3 ACL INPUT Statistics
  Drop: All frame count: 0
  Drop: All bytes count: 0
  Drop And Log: All frame count: 0
  Drop And Log: All bytes count: 0
  Bridge Only: All frame count: 0
  Bridge Only: All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU: All frame count: 0
  Forwarding To CPU: All bytes count: 0
  Forwarded: All frame count: 13586
  Forwarded: All bytes count: 1236182
  Forwarded And Log: All frame count: 0
  Forwarded And Log: All bytes count: 0
```



```

L2 ACL OUTPUT Statistics
Drop: All frame count: 0
Drop: All bytes count: 0
Drop And Log: All frame count: 0
Drop And Log: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Bridge Only And Log: All frame count: 0
Bridge Only And Log: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0
Forwarded: All frame count: 232983
Forwarded: All bytes count: 16825661
Forwarded And Log: All frame count: 0
Forwarded And Log: All bytes count: 0

L3 ACL OUTPUT Statistics
Drop: All frame count: 0
Drop: All bytes count: 0
Drop And Log: All frame count: 0
Drop And Log: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Bridge Only And Log: All frame count: 0
Bridge Only And Log: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0
Forwarded: All frame count: 514434
Forwarded: All bytes count: 39048748
Forwarded And Log: All frame count: 0
Forwarded And Log: All bytes count: 0

```

関連コマンド

コマンド	説明
access-list	スイッチに標準または拡張番号アクセス リストを設定します。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。
ip access-list	スイッチに指定された IP アクセス リストを設定します。構文情報については、「Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2」>「IP Services Commands」を選択してください。
mac access-list extended	スイッチに、指定されたまたは番号のついた MAC (メディア アクセス制御) アクセス リストを設定します。

show archive status

HTTP または TFTP プロトコルでスイッチにダウンロードされた新しいイメージのステータスを表示するには、**show archive status** 特権 EXEC コマンドを使用します。

```
show archive status [ | {begin | exclude | include} expression]
```

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

archive download-sw 特権 EXEC コマンドを使用してイメージを TFTP サーバにダウンロードする場合、**archive download-sw** コマンドの出力では、ダウンロードのステータスが表示されます。

TFTP サーバがない場合、HTTP を使用してイメージをダウンロードするには、**Network Assistant** または組み込みデバイス マネージャを使用します。**show archive status** コマンドでは、ダウンロードの進捗状況が表示されます。

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 次の例では、**show archive status** コマンドの出力を示します。

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

関連コマンド

コマンド	説明
archive download-sw	TFTP サーバからスイッチに新しいイメージをダウンロードします。

show arp access-list

アドレス解決プロトコル (ARP) アクセスコントロールリスト (1 つまたは複数) の詳細を表示するには、**show arp access-list** ユーザ EXEC コマンドを使用します。

```
show arp access-list [acl-name] [| {begin | exclude | include} expression]
```

シンタックスの説明

<i>acl-name</i>	(任意) ACL の名前です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show arp access-list** コマンドの出力を示します。

```
Switch> show arp access-list
ARP access list rose
  permit ip 10.101.1.1 0.0.0.255 mac any
  permit ip 20.3.1.0 0.0.0.255 mac any
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
deny (ARP アクセス リスト コンフィギュレーション)	Dynamic Host Configuration Protocol (DHCP) バインディングと一致した ARP パケットを拒否します。
ip arp inspection filter vlan	スタティック IP アドレスが設定されたホストからの ARP 要求と ARP 応答を許可します。
permit (ARP アクセス リスト コンフィギュレーション)	DHCP バインディングと一致した ARP パケットを許可します。

show authentication

スイッチ上の認証マネージャ イベントに関する情報を表示するには、**show authentication** コマンド (ユーザ EXEC モードまたは特権 EXEC モードのいずれか) を使用します。

show authentication {interface *interface-id* | registrations | sessions [session-id session-id] [handle *handle*] [interface *interface-id*] [mac *mac*] [method *method*]}

シンタックスの説明

interface <i>interface-id</i>	(任意) 指定したインターフェイスの認証マネージャ詳細をすべて表示します。
method <i>method</i>	(任意) 特定の認証方式 (dot1x 、 mab 、または webauth) で許可されたクライアントをすべて表示します。
registrations	(任意) 認証マネージャのレジストレーションを表示します。
sessions	(任意) 現在の認証マネージャセッションの詳細 (クライアントデバイスなど) を表示します。任意の指定子を入力しないと、現在アクティブなセッションがすべて表示されます。1 つの指定子を入力して特定のセッションを表示するか、または指定子の組み合わせを入力して 1 組のセッションを表示することができます。
session-id <i>session-id</i>	(任意) 認証マネージャセッションを指定します。
handle <i>handle</i>	(任意) 1 ~ 4294967295 の範囲を指定します。
mac <i>mac</i>	(任意) 特定の MAC アドレスの認証マネージャ情報を表示します。

コマンドのデフォルト

このコマンドには、デフォルト設定はありません。

コマンドモード

特権 EXEC およびユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

表 2-18 に、**show authentication** コマンドの出力に表示される重要なフィールドを示します。



(注)

セッションのステートとして表示される可能性のある値を次に示します。終端ステートのセッションでは、結果を生成する方式が存在しない場合に *No methods* と同時に *Authz Success* または *Authz Failed* が表示されます。

表 2-18 show authentication コマンドの出力

フィールド	説明
Idle	該当するセッションがすでに初期化されており、どの方式もまだ実行されていません。
Running	該当するセッションに対して 1 つの方式が実行されています。

表 2-18 show authentication コマンドの出力 (続き)

フィールド	説明
No methods	該当するセッションに対して結果を生成する方式が存在しません。
Authc Success	1つの方式により、該当するセッションの認証に成功しました。
Authc Failed	1つの方式により、該当するセッションの認証に失敗しました。
Authz Success	該当するセッションへのすべての機能の適用に成功しました。
Authz Failed	該当するセッションへの機能の適用に失敗しました。

表 2-19 に、方式のステートとして表示される可能性のある値を示します。終端ステートのセッションでは、*Authc Success*、*Authc Failed*、または *Failed over* が表示されます。*Failed over* は、ある認証方式が実行されたあとで次の方式にフェールオーバーされたことを示します (結果は生成されません)。*Not run* は、スタンバイ上で同期化されたセッションに対して表示されます。

表 2-19 方式のステートを表す値

方式のステート	ステートのレベル	説明
Not run	終端	該当するセッションに対してこの方式が実行されていません。
Running	中間	該当するセッションに対してこの方式が実行されています。
Failed over	終端	この方式に失敗したため、次の方式で結果が生成されることとなります。
Authc Success	終端	この方式により、該当するセッションの認証に成功しました。
Authc Failed	終端	この方式により、該当するセッションの認証に失敗しました。

例

次の例では、**show authentication registrations** コマンドの出力を示します。

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
Handle Priority Name
3 0 dot1x
2 1 mab
1 2 webauth
```

次の例では、**show authentication interface interface-id** コマンドの出力を示します。

```
Switch# show authentication interface gigabitethernet1/23
Client list:
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/0/23
Available methods list:
Handle Priority Name
3 0 dot1x
Runnable methods list:
Handle Priority Name
3 0 dot1x
```

次の例では、**show authentication sessions** コマンドの出力を示します。

```
Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
Gi3/45 (unknown) N/A DATA Authz Failed 0908140400000007003651EC
Gi3/46 (unknown) N/A DATA Authz Success 09081404000000080057C274
```

次の例では、特定のインターフェイスに対する **show authentication sessions** コマンドの出力を示します。

```
Switch# show authentication sessions int gi 3/46
      Interface: GigabitEthernet3/46
      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: 4094
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0908140400000080057C274
      Acct Session ID: 0x0000000A
      Handle: 0xCC000008
      Runnable methods list:
      Method State
      dot1x Failed over
```

次の例では、特定の MAC アドレスに対する **show authentication sessions** コマンドの出力を示します。

```
Switch# show authentication sessions mac 000e.84af.59bd
Interface: GigabitEthernet1/23
MAC Address: 000e.84af.59bd
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
```

次の例では、特定の方式に対する **show authentication session method** コマンドの出力を示します。

```
Switch# show authentication sessions method mab
No Auth Manager contexts match supplied criteria
Switch# show authentication sessions method dot1x
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/23
```

関連コマンド

コマンド	説明
authentication control-direction	ポートを単一方向モードまたは双方向モードに設定します。
authentication event	特定の認証イベントに対するアクションを設定します。
authentication host-mode	ポート上で認証マネージャ モードを設定します。
authentication open	ポート上でオープン 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	ポート上で使用される認証方式の順序を設定します。
authentication periodic	ポート上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	ポートの許可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された場合、またはすでに最大数のデバイスがポートに接続されている状態で新規のデバイスがそのポートに接続された場合に適用される違反モードを設定します。

show auto qos

Automatic QoS (auto-QoS) がイネーブルのインターフェイスで入力された QoS (Quality of Service) コマンドを表示するには、**show auto qos** ユーザ EXEC コマンドを使用します。

show auto qos [interface [interface-id]]



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

interface [interface-id]	(任意) 指定されたポートまたはすべてのポートの auto-QoS 情報を表示します。指定できるインターフェイスとして、物理ポートも含まれます。
---------------------------------	--

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(40)SE	コマンド出力の情報が変更されました。

使用上のガイドライン

show auto qos コマンドの出力には、各インターフェイスで入力された auto-QoS コマンドだけが表示されます。**show auto qos interface interface-id** コマンド出力は、特定のインターフェイスに入力された auto-QoS コマンドを表示します。

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。

show auto qos コマンドの出力には、Cisco IP Phone のサービス ポリシー情報も表示されます。

auto-QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface [interface-id] [buffers | queueing]**
- **show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-output-q]**
- **show mls qos input-queue**
- **show running-config**

例

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。

```
Switch> show auto qos
GigabitEthernet0/4
```



```
auto qos voip cisco-softphone
```

```
GigabitEthernet0/5
auto qos voip cisco-phone
```

```
GigabitEthernet0/6
auto qos voip cisco-phone
```

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface interface-id** コマンドの出力を示します。

```
Switch> show auto qos interface gigabitethernet 0/5
GigabitEthernet0/5
auto qos voip cisco-phone
```

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 running-config** 特権 EXEC コマンドの出力を示します。

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 75 75 75 250
mls qos queue-set output 1 threshold 3 75 150 100 300
mls qos queue-set output 1 threshold 4 50 100 75 400
mls qos queue-set output 2 threshold 1 100 100 100 100
mls qos queue-set output 2 threshold 2 35 35 35 35
mls qos queue-set output 2 threshold 3 55 82 100 182
```

show auto qos

```
mls qos queue-set output 2 threshold 4 90 250 100 400
mls qos queue-set output 1 buffers 15 20 20 45
mls qos queue-set output 2 buffers 24 20 26 30
mls qos
...
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3 af31
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
!
policy-map AutoQoS-Police-CiscoPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
...
!
interface GigabitEthernet0/4
  switchport mode access
  switchport port-security maximum 400
  service-policy input AutoQoS-Police-SoftPhone
  speed 100
  duplex half
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  auto qos voip cisco-softphone
!
interface GigabitEthernet0/5
  switchport mode access
  switchport port-security maximum 1999
  speed 100
  duplex full
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
!
interface GigabitEthernet0/6
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 2
  switchport mode access
  speed 10
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
!
interface GigabitEthernet0/1
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
```

```
mls qos trust cos
mls qos trust device cisco-phone
service-policy input AutoQoS-Police-CiscoPhone
```

<output truncated>

次の例では、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos interface interface-id** コマンドの出力を示します。

```
Switch> show auto qos interface fastethernet0/2
FastEthernet0/2
auto qos voip cisco-softphone
```

次の例では、スイッチ上で Auto-QoS がディセーブルになっている場合の **show auto qos** コマンドの出力を示します。

```
Switch> show auto qos
AutoQoS not enabled on any interface
```

次の例では、Auto-QoS がインターフェイスでディセーブルの場合の **show auto qos interface interface-id** コマンドの出力を示します。

```
Switch> show auto qos interface gigabitethernet0/1
AutoQoS is disabled
```

関連コマンド

コマンド	説明
auto qos voip	QoS ドメイン内の Voice over IP (VoIP) に QoS を自動設定します。
debug auto qos	Auto-QoS 機能のデバッグをイネーブルにします。

show boot

BOOT 環境変数の設定を表示するには、**show boot** 特権 EXEC コマンドを使用します。

show boot [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show boot** コマンドの出力を示します。表 2-20 に、表示される各フィールドの説明を示します。

```
Switch# show boot
BOOT path-list: flash:c2960-lanbase-mz.122-25.FX.bin
Config file:      flash:/config.text
Private Config file: flash:/private-config
Enable Break:    no
Manual Boot:     yes
HELPER path-list:
NVRAM/Config file
      buffer size: 32768
```

表 2-20 show boot の出力に表示される各フィールドの説明

フィールド	説明
BOOT path-list	自動起動時にロードおよび実行しようとする実行可能ファイルのセミコロン区切りリストを表示します。 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、最初に見つかった実行可能イメージをロードして実行しようとしています。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。 BOOT 環境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い場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとしています。
Config file	Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。
Private Config file	Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を表示します。
Enable Break	起動中のブレイクがイネーブルか、またはディセーブルかを表示します。yes、on、または 1 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 キーを押すと、自動起動プロセスを中断できます。
Manual Boot	スイッチが自動で起動するか、または手動で起動するかを表示します。no または 0 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ようとしています。他の値に設定されている場合は、ブート ローダ モードから手動でスイッチを起動する必要があります。
Helper path-list	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表示します。ヘルパー ファイルは、ブート ローダの機能を拡張したり、パッチを当てます。
NVRAM/Config ファイルのバッファ サイズ	Cisco IOS がメモリ内のコンフィギュレーション ファイルのコピーを保持するために使用するバッファ サイズを表示します。コンフィギュレーション ファイルは、バッファ サイズ割り当てを超えることはできません。

関連コマンド

コマンド	説明
boot 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指定します。
boot enable-break	自動起動プロセスを中断できます。
boot manual	次の起動サイクル時の手動スイッチ起動をイネーブルにします。
boot private-config-file	Cisco IOS がプライベート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。
boot system	次の起動サイクル中にロードする Cisco IOS イメージを指定します。

show cable-diagnostics tdr

Time Domain Reflector (TDR) 結果を表示するには、**show cable-diagnostics tdr** 特権 EXEC コマンドを使用します。

```
show cable-diagnostics tdr interface interface-id [| {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	TDR が実行されているインターフェイスを指定します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。SFP モジュールポートではサポートされません。TDR の詳細については、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。

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

次の例では、**show cable-diagnostics tdr interface *interface-id*** コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length          Remote pair Pair status
-----
Gi0/2      auto  Pair A    0    +/- 2 meters N/A          Open
                Pair B    0    +/- 2 meters N/A          Open
                Pair C    0    +/- 2 meters N/A          Open
                Pair D    0    +/- 2 meters N/A          Open
```

表 2-21 に、**show cable-diagnostics tdr** コマンドの出力に表示される各フィールドの説明を示します。

表 2-21 show cable-diagnostics tdr コマンドでの出力されるフィールドの説明

フィールド	説明
Interface	TDR が実行されたインターフェイス
Speed	接続速度
Local pair	ローカル インターフェイスで TDR がテストを実行するワイヤ ペア名

表 2-21 show cable-diagnostics tdr コマンドでの出力されるフィールドの説明 (続き)

フィールド	説明
Pair length	<p>使用するスイッチについて、問題が発生したケーブルの場所。次の場合に、TDR は場所を特定します。</p> <ul style="list-style-type: none"> • ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が 1000Mb/s である場合 • ケーブルが断線している場合 • ケーブルがショートしている場合
Remote pair	ローカル ペアが接続されたワイヤ ペア名。ケーブルが正しく接続されリンクがアップ状態である場合にのみ、TDR はリモート ペアについて確認します。
Pair status	<p>TDR が稼動しているワイヤ ペアのステータス</p> <ul style="list-style-type: none"> • Normal : ワイヤ ペアが正しく接続されています。 • Not completed : テストが実行され、まだ完了していません。 • Not supported : インターフェイスは TDR をサポートしません。 • Open : ワイヤ ペアが断線しています。 • Shorted : ワイヤ ペアがショートしています。 • ImpedanceMis : インピーダンスが一致しません。 • Short/Impedance Mismatched : インピーダンスが一致していないか、ケーブルの長さが足りません。 • InProgress : 診断テストが実行中です。

次の例では、TDR が動作している場合の **show interfaces interface-id** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/2
gigabitethernet0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が動作していない場合の **show cable-diagnostics tdr interface interface-id** コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
% TDR test was never issued on Gi0/2
```

インターフェイスで TDR がサポートされていない場合は、次のメッセージが表示されます。

```
% TDR test is not supported on switch 1
```

関連コマンド

コマンド	説明
test cable-diagnostics tdr	インターフェイスで TDR をイネーブルにし、実行します。

show cisp

特定のインターフェイスの CISP 情報を表示するには、**show cisp** 特権 EXEC コマンドを使用します。

```
show cisp {[interface interface-id] | clients | summary} | {[begin | exclude | include]
expression}}
```

シンタックスの説明

clients	(任意) CISP クライアントの詳細を表示します。
interface interface-id	(任意) 指定したインターフェイスの CISP 情報を表示します。有効なインターフェイスは、物理ポートおよびポート チャネルです。
summary	(任意) 概要を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、**show cisp interface** コマンドの出力を示します。

```
WS-C3750E-48TD#show cisp interface fast 0
CISP not enabled on specified interface
```

次の例では、**show cisp summary** コマンドの出力を示します。

```
CISP is not running on any interface
```

関連コマンド

コマンド	説明
dot1x credentials profile	サブリカント スイッチのプロファイルを設定します。
cisp enable	Client Information Signalling Protocol (CISP) をイネーブ ルにします。

show class-map

show class-map ユーザ EXEC コマンドは、トラフィックを分類するための一致基準を定義する QoS (Quality of Service) クラス マップを表示します。

show class-map [*class-map-name*] [| {**begin** | **exclude** | **include**} *expression*]



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>class-map-name</i>	(任意) 指定されたクラス マップの内容を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show class-map** コマンドの出力を示します。

```
Switch> show class-map
Class Map match-all 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-all dscp5 (id 3)
  Match ip dscp 5
```

関連コマンド

コマンド	説明
class-map	名前を指定したクラスとパケットとの比較に使用されるクラス マップを作成します。
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条件を定義します。

show cluster

スイッチが属しているクラスタのステータスとサマリーを表示するには、**show cluster** ユーザ EXEC コマンドを使用します。このコマンドは、クラスタ コマンド スイッチとクラスタ メンバー スイッチでのみ入力できます。

show cluster [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

クラスタのメンバーでないスイッチ上でこのコマンドを入力すると、エラー メッセージ `Not a management cluster member` が表示されます。

クラスタ メンバー スイッチ上でこのコマンドを入力すると、クラスタ コマンド スイッチの ID、そのスイッチ メンバーの番号、およびクラスタ コマンド スイッチとの接続状態が表示されます。

クラスタ コマンド スイッチ上でこのコマンドを入力すると、クラスタ名およびメンバーの総数が表示されます。また、ステータス変更後のクラスタのステータスおよび時間も表示されます。冗長構成がイーネーブルの場合は、プライマリおよびセカンダリ コマンド スイッチの情報が表示されます。

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

次の例では、アクティブなクラスタ コマンド スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "Ajang"
  Total number of members:          7
  Status:                          1 members are unreachable
  Time since last status change:    0 days, 0 hours, 2 minutes
  Redundancy:                       Enabled
    Standby command switch: Member 1
    Standby Group:                  Ajang_standby
    Standby Group Number:          110
  Heartbeat interval:               8
  Heartbeat hold-time:              80
  Extended discovery hop count:     3
```

次の例では、クラスタ メンバー スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch1> show cluster
Member switch for cluster "hapuna"
  Member number:          3
  Management IP address:  192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:     8
  Heartbeat hold-time:    80
```

次の例では、スタンバイ クラスタ コマンド スイッチとして設定されたクラスタ メンバー スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
  Member number:          3 (Standby command switch)
  Management IP address:  192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:     8
  Heartbeat hold-time:    80
```

次の例では、メンバー 1 との接続が切断されたクラスタ コマンド スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Command switch for cluster "Ajang"
  Total number of members: 7
  Status:                  1 members are unreachable
  Time since last status change: 0 days, 0 hours, 5 minutes
  Redundancy:              Disabled
  Heartbeat interval:      8
  Heartbeat hold-time:     80
  Extended discovery hop count: 3
```

次の例では、クラスタ コマンド スイッチとの接続が切断されたクラスタ メンバー スイッチ上で **show cluster** コマンドを入力した場合の出力を示します。

```
Switch> show cluster
Member switch for cluster "hapuna"
  Member number:          <UNKNOWN>
  Management IP address:  192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:     8
  Heartbeat hold-time:    80
```

関連コマンド

コマンド	説明
cluster enable	コマンド対応スイッチをクラスタ コマンド スイッチとしてイネーブルにし、クラスタ名、およびオプションとしてメンバー番号を割り当てます。
show cluster candidates	候補スイッチのリストを表示します。
show cluster members	クラスタ メンバーに関する情報を表示します。

show cluster candidates

候補スイッチのリストを表示するには、**show cluster candidates** 特権 EXEC コマンドを使用します。

```
show cluster candidates [detail | mac-address H.H.H.] [ | {begin | exclude | include}
expression]
```

シンタックスの説明

detail	(任意) すべての候補に関する詳細を表示します。
mac-address H.H.H.	(任意) クラスタ候補の MAC (メディア アクセス制御) アドレスです。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でのみ利用できます。

スイッチがクラスタ コマンド スイッチでない場合は、プロンプトに空行が表示されます。

出力内の SN は、スイッチメンバー番号を意味します。SN 列の値に E が表示された場合、スイッチは拡張検出によって検出されています。SN 列の値が E でない場合、スイッチメンバー番号のスイッチは、候補スイッチのアップストリーム側ネイバーです。ホップ数は、クラスタ コマンド スイッチから候補スイッチまでのデバイス数です。

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

次の例では、**show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates
                                     |---Upstream---|
MAC Address      Name           Device Type      PortIf  FEC Hops SN PortIf  FEC
00d0.7961.c4c0  StLouis-2     WS-C2960-12T    Gi0/1   2   1   1 Fa0/11
00d0.bbf5.e900  ldf-dist-128 WS-C3524-XL     Fa0/7   1   0   0 Fa0/24
00e0.1e7e.be80  1900_Switch  1900            3       0   1   0 Fa0/11
00e0.1e9f.7a00  Surfers-24   WS-C2924-XL     Fa0/5   1   0   0 Fa0/3
00e0.1e9f.8c00  Surfers-12-2 WS-C2912-XL     Fa0/4   1   0   0 Fa0/7
00e0.1e9f.8c40  Surfers-12-1 WS-C2912-XL     Fa0/1   1   0   0 Fa0/9
```

次の例では、クラスタ コマンド スイッチに直接接続された、クラスタ メンバー スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 00d0.7961.c4c0
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
  Device type:                cisco WS-C2960-12T
  Upstream MAC address:       00d0.796d.2f00 (Cluster Member 0)
  Local port:                 Gi0/1    FEC number:
  Upstream port:              GI0/11   FEC Number:
Hops from cluster edge: 1
  Hops from command device: 1
```

次の例では、クラスタ エッジからのホップ数が 3 である、クラスタ メンバー スイッチの MAC アドレスを使用した場合の **show cluster candidates** コマンドの出力を示します。

```
Switch> show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
  Device type:                cisco WS-C2912MF-XL
  Upstream MAC address:       0010.7bb6.1cd4
  Local port:                 Fa2/1    FEC number:
  Upstream port:              Fa0/24   FEC Number:
Hops from cluster edge: 3
  Hops from command device: -
```

次の例では、**show cluster candidates detail** コマンドの出力を示します。

```
Switch> show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
  Device type:                cisco WS-C3512-XL
  Upstream MAC address:       00d0.796d.2f00 (Cluster Member 1)
  Local port:                 Fa0/3    FEC number:
  Upstream port:              Fa0/13   FEC Number:
Hops from cluster edge: 1
  Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
  Device type:                cisco 1900
  Upstream MAC address:       00d0.796d.2f00 (Cluster Member 2)
  Local port:                 3        FEC number: 0
  Upstream port:              Fa0/11   FEC Number:
Hops from cluster edge: 1
  Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
  Device type:                cisco WS-C2924-XL
  Upstream MAC address:       00d0.796d.2f00 (Cluster Member 3)
  Local port:                 Fa0/5    FEC number:
  Upstream port:              Fa0/3    FEC Number:
Hops from cluster edge: 1
  Hops from command device: 2
```

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster members	クラスタ メンバーに関する情報を表示します。

show cluster members

クラスタ メンバーの情報を表示するには、**show cluster members** 特権 EXEC コマンドを使用します。

show cluster members [*n* | **detail**] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>n</i>	(任意) クラスタ メンバーを識別する番号。指定できる範囲は 0 ~ 15 です。
detail	(任意) すべてのクラスタ メンバーに関する詳細を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でのみ利用できます。

クラスタ内にメンバーがない場合は、プロンプトに空行が表示されます。

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

次の例では、**show cluster members** コマンドの出力を示します。出力内の SN は、スイッチ番号を意味します。

```
Switch# show cluster members

```

---Upstream---									
SN	MAC Address	Name	PortIf	FEC	Hops	SN	PortIf	FEC	State
0	0002.4b29.2e00	StLouis1			0				Up (Cmdr)
1	0030.946c.d740	tal-switch-1	Fa0/13		1	0	Gi0/1		Up
2	0002.b922.7180	nms-2820	10	0	2	1	Fa0/18		Up
3	0002.4b29.4400	SanJuan2	Gi0/1		2	1	Fa0/11		Up
4	0002.4b28.c480	GenieTest	Gi0/2		2	1	Fa0/9		Up

次の例では、クラスタ メンバー 3 に対する **show cluster members** の出力を示します。

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
Device type:          cisco WS-C2960
MAC address:          0002.4b29.4400
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:           Gi0/1   FEC number:
Upstream port:        GI0/11  FEC Number:
Hops from command device: 2
```

次の例では、**show cluster members detail** コマンドの出力を示します。

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
  Device type:          cisco WS-C2960
  MAC address:          0002.4b29.2e00
  Upstream MAC address:
  Local port:           FEC number:
  Upstream port:        FEC Number:
  Hops from command device: 0
Device 'tal-switch-14' with member number 1
  Device type:          cisco WS-C3548-XL
  MAC address:          0030.946c.d740
  Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
  Local port:           Fa0/13  FEC number:
  Upstream port:        Gi0/1   FEC Number:
  Hops from command device: 1
Device 'nms-2820' with member number 2
  Device type:          cisco 2820
  MAC address:          0002.b922.7180
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:           10      FEC number: 0
  Upstream port:        Fa0/18  FEC Number:
  Hops from command device: 2
Device 'SanJuan2' with member number 3
  Device type:          cisco WS-C2960
  MAC address:          0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:           Gi0/1   FEC number:
  Upstream port:        Fa0/11  FEC Number:
  Hops from command device: 2
Device 'GenieTest' with member number 4
  Device type:          cisco SeaHorse
  MAC address:          0002.4b28.c480
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:           Gi0/2   FEC number:
  Upstream port:        Fa0/9   FEC Number:
  Hops from command device: 2
Device 'Palpatine' with member number 5
  Device type:          cisco WS-C2924M-XL
  MAC address:          00b0.6404.f8c0
  Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
  Local port:           Gi2/1   FEC number:
  Upstream port:        Gi0/7   FEC Number:
  Hops from command device: 1
```

関連コマンド

コマンド	説明
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	候補スイッチのリストを表示します。

show controllers cpu-interface

CPU ネットワーク インターフェイス ASIC（特定用途向け集積回路）のステータスを表示し、CPU に達するパケットに関する統計情報を送受信するには、**show controllers cpu-interface** 特権 EXEC コマンドを使用します。

show controllers cpu-interface [| { **begin** | **exclude** | **include** } *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用することで、シスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ情報が表示されます。

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

次の例では、**show controllers cpu-interface** コマンドの出力を示します。

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped  invalid  hol-block
-----
rpc                4523063    0        0        0
stp                1545035    0        0        0
ipc                1903047    0        0        0
routing protocol  96145      0        0        0
L2 protocol        79596      0        0        0
remote console     0          0        0        0
sw forwarding      5756       0        0        0
host               225646     0        0        0
broadcast          46472      0        0        0
cbt-to-spt         0          0        0        0
igmp snooping      68411      0        0        0
icmp               0          0        0        0
logging            0          0        0        0
rpf-fail           0          0        0        0
queue14            0          0        0        0
cpu heartbeat      1710501    0        0        0

Supervisor ASIC receive-queue parameters
-----
queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
```



```

queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
queue 3 maxrecevsize 5EE pakhead 19CDDD0 paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----
MicDirectPollInfo          80000800
MicIndicationsReceived     00000000
MicInterruptsReceived     00000000
MicPcsInfo                 0001001F
MicPlbMasterConfiguration 00000000
MicRxFifosAvailable       00000000
MicRxFifosReady           0000BFFF
MicTimeOutPeriod:         FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

<output truncated>

MicTransmitFifoInfo:
Fifo0:  StartPtrs:      038C2800      ReadPtr:      038C2C38
        WritePtrs:      038C2C38      Fifo_Flag:    8A800800
        Weights:        001E001E
Fifo1:  StartPtr:      03A9BC00      ReadPtr:      03A9BC60
        WritePtrs:      03A9BC60      Fifo_Flag:    89800400
        writeHeaderPtr: 03A9BC60
Fifo2:  StartPtr:      038C8800      ReadPtr:      038C88E0
        WritePtrs:      038C88E0      Fifo_Flag:    88800200
        writeHeaderPtr: 038C88E0
Fifo3:  StartPtr:      03C30400      ReadPtr:      03C30638
        WritePtrs:      03C30638      Fifo_Flag:    89800400
        writeHeaderPtr: 03C30638
Fifo4:  StartPtr:      03AD5000      ReadPtr:      03AD50A0
        WritePtrs:      03AD50A0      Fifo_Flag:    89800400
        writeHeaderPtr: 03AD50A0
Fifo5:  StartPtr:      03A7A600      ReadPtr:      03A7A600
        WritePtrs:      03A7A600      Fifo_Flag:    88800200
        writeHeaderPtr: 03A7A600
Fifo6:  StartPtr:      03BF8400      ReadPtr:      03BF87F0
        WritePtrs:      03BF87F0      Fifo_Flag:    89800400

<output truncated>

```

関連コマンド

コマンド	説明
show controllers ethernet-controller	ハードウェアまたはインターフェイスの内部レジスタから読み込まれる、各インターフェイスの送受信の統計情報を表示します。
show interfaces	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管理ステータスおよび動作ステータスを表示します。

show controllers ethernet-controller

ハードウェアから読み込んだ送受信に関するインターフェイス単位の統計情報をキーワードなしで表示するには、**show controllers ethernet-controller** 特権 EXEC コマンドを使用します。**phy** キーワードはインターフェイス内部レジスタを表示し、**port-asic** キーワードはポート ASIC（特定用途向け集積回路）に関する情報を表示します。

```
show controllers ethernet-controller [interface-id] [phy [detail]] [port-asic
{configuration | statistics}] [fastethernet 0][ | {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	物理インターフェイス（タイプ、モジュール、ポート番号を含む）
phy	（任意）デバイス、またはインターフェイスのスイッチの物理層（PHY）デバイスの内部レジスタ ステータスを表示します。インターフェイスの Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能の動作ステータスを表示に含めます。
detail	（任意）PHY 内部レジスタの詳細情報を表示します。
port-asic	（任意）ポートの ASIC 内部レジスタの情報を表示します。
configuration	ポートの ASIC 内部レジスタの設定を表示します。
statistics	ポートの ASIC 統計情報（Rx/Sup キューおよびその他の統計情報を含む）を表示します。
begin	（任意） <i>expression</i> と一致する行から表示を開始します。
exclude	（任意） <i>expression</i> と一致する行を表示から除外します。
include	（任意）指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC（ユーザ EXEC モードの *interface-id* キーワードでのみサポート）

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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基本的な RMON 統計情報を含むトラブルシューティング統計情報をキーワードなしで表示します。

phy または **port-asic** キーワードを入力した場合は、主にシスコのテクニカル サポート担当のスイッチのトラブルシューティングに役立つ情報が表示されます。

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

次の例では、特定のインターフェイスに対する **show controllers ethernet-controller** コマンドの出力を示します。表 2-22 に *Transmit* の各フィールドの説明を示し、表 2-23 に *Receive* の各フィールドの説明を示します。

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1
  0 Bytes
  0 Unicast frames
  0 Multicast frames
  0 Broadcast frames
  0 Too old frames
  0 Deferred frames
  0 MTU exceeded frames
  0 1 collision frames
  0 2 collision frames
  0 3 collision frames
  0 4 collision frames
  0 5 collision frames
  0 6 collision frames
  0 7 collision frames
  0 8 collision frames
  0 9 collision frames
  0 10 collision frames
  0 11 collision frames
  0 12 collision frames
  0 13 collision frames
  0 14 collision frames
  0 15 collision frames
  0 Excessive collisions
  0 Late collisions
  0 VLAN discard frames
  0 Excess defer frames
  0 64 byte frames
  0 127 byte frames
  0 255 byte frames
  0 511 byte frames
  0 1023 byte frames
  0 1518 byte frames
  0 Too large frames
  0 Good (1 coll) frames
Receive
  0 Bytes
  0 Unicast frames
  0 Multicast frames
  0 Broadcast frames
  0 Unicast bytes
  0 Multicast bytes
  0 Broadcast bytes
  0 Alignment errors
  0 FCS errors
  0 Oversize frames
  0 Undersize frames
  0 Collision fragments
  0 Minimum size frames
  0 65 to 127 byte frames
  0 128 to 255 byte frames
  0 256 to 511 byte frames
  0 512 to 1023 byte frames
  0 1024 to 1518 byte frames
  0 Overrun frames
  0 Pause frames
  0 Symbol error frames
  0 Invalid frames, too large
  0 Valid frames, too large
  0 Invalid frames, too small
  0 Valid frames, too small
  0 Too old frames
  0 Valid oversize frames
  0 System FCS error frames
  0 RxPortFifoFull drop frame
```

表 2-22 Transmit のフィールドの説明

フィールド	説明
Bytes	インターフェイス上で送信されたバイトの総数。
Unicast Frames	ユニキャスト アドレスに送信されたフレームの総数。
Multicast frames	マルチキャスト アドレスに送信されたフレームの総数。
Broadcast frames	ブロードキャスト アドレスに送信されたフレームの総数。
Too old frames	パケットが有効期限切れのため出力ポートでドロップされたフレームの数。
Deferred frames	時間が 2* 最大パケット時間を超えたあとで送信されなかったフレームの数。
MTU exceeded frames	最大許可フレーム サイズを超えたフレームの数。
1 collision frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
2 collision frames	2 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
3 collision frames	3 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
4 collision frames	4 回の衝突後、インターフェイス上で正常に送信されたフレームの数。

表 2-22 Transmit のフィールドの説明 (続き)

フィールド	説明
5 collision frames	5 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
6 collision frames	6 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
7 collision frames	7 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
8 collision frames	8 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
9 collision frames	9 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
10 collision frames	10 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
11 collision frames	11 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
12 collision frames	12 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
13 collision frames	13 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
14 collision frames	14 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
15 collision frames	15 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
Excessive collisions	16 回の衝突後、インターフェイス上で送信できなかったフレームの数。
Late collisions	フレームが送信されたあとで、フレームの送信時に検出されたレイト コリジョンによってドロップされたフレームの数。
VLAN discard frames	CFI ¹ ビットが設定されたことによりインターフェイス上でドロップされたフレームの数。
Excess defer frames	時間が最大パケット時間を超えたあとで送信されなかったフレームの数。
64 byte frames	インターフェイス上で送信された 64 バイトのフレームの総数。
127 byte frames	インターフェイス上で送信された 65 ~ 127 バイトのフレームの総数。
255 byte frames	インターフェイス上で送信された 128 ~ 255 バイトのフレームの総数。
511 byte frames	インターフェイス上で送信された 256 ~ 511 バイトのフレームの総数。
1023 byte frames	インターフェイス上で送信された 512 ~ 1023 バイトのフレームの総数。
1518 byte frames	インターフェイス上で送信された 1024 ~ 1518 バイトのフレームの総数。
Too large frames	インターフェイス上で送信された最大許可フレーム サイズを超えたフレームの数。
Good (1 coll) frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。この値には 1 回の衝突後、インターフェイス上で正常に送信されなかったフレームの数は含まれません。

1. CFI = Canonical Format Indicator (フォーマット形式表示)

表 2-23 Receive のフィールドの説明

フィールド	説明
Bytes	インターフェイス上で受信されたフレームによって使用されたメモリ (バイト) の総量。FCS ¹ 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Unicast frames	インターフェイス上で正常に受信されたユニキャスト アドレスに向けられたフレームの総数。
Multicast frames	インターフェイス上で正常に受信されたマルチキャスト アドレスに向けられたフレームの総数。
Broadcast frames	インターフェイス上で正常に受信されたブロードキャスト アドレスに向けられたフレームの総数。
Unicast bytes	インターフェイス上で受信されたユニキャスト フレームによって使用されたメモリ (バイト) の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。

表 2-23 Receive のフィールドの説明 (続き)

フィールド	説明
Multicast bytes	インターフェイス上で受信されたマルチキャスト フレームによって使用されたメモリ (バイト) の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Broadcast bytes	インターフェイス上で受信されたブロードキャスト フレームによって使用されたメモリ (バイト) の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Alignment errors	インターフェイス上で受信されたアライメント エラーを持つフレームの総数。
FCS errors	インターフェイス上で受信された有効な長さ (バイト) を持ち、正常な FCS 値を持たないフレームの総数。
Oversize frames	インターフェイス上で受信された最大許可フレーム サイズを超えたフレームの数。
Undersize frames	インターフェイス上で受信された 64 バイト未満のフレームの数。
Collision fragments	インターフェイス上で受信されたコリジョン フラグメントの数。
Minimum size frames	最小フレーム サイズのフレームの総数。
65 to 127 byte frames	65 ~ 127 バイトのフレームの総数。
128 to 255 byte frames	128 ~ 255 バイトのフレームの総数。
256 to 511 byte frames	256 ~ 511 バイトのフレームの総数。
512 to 1023 byte frames	512 ~ 1023 バイトのフレームの総数。
1024 to 1518 byte frames	1024 ~ 1518 バイトのフレームの総数。
Overrun frames	インターフェイス上で受信されたオーバーラン フレームの総数。
Pause frames	インターフェイス上で受信されたポーズ フレームの数。
Symbol error frames	インターフェイス上で受信されたシンボル エラーを持つフレームの数。
Invalid frames, too large	許可 MTU ² サイズ (FCS ビットを含み、フレーム ヘッダーを含まない) を超え、FCS エラーまたはアライメント エラーのどちらかを持つ受信されたフレームの数。
Valid frames, too large	インターフェイス上で受信された最大許可フレーム サイズを超えたフレームの数。
Invalid frames, too small	64 バイト (FCS ビットを含み、フレーム ヘッダーを含まない) 未満で、FCS エラーまたはアライメント エラーのどちらかを持つ受信されたフレームの数。
Valid frames, too small	64 バイト (または VLAN タグ付きフレームでは 68 バイト) 未満で、有効な FCS 値を持つインターフェイスで受信されたフレームの数。フレーム サイズには、FCS ビットが含まれ、フレーム ヘッダー ビットは含まれません。
Too old frames	パケットが有効期限切れのため入力ポートでドロップされたフレームの数。
Valid oversize frames	インターフェイス上で受信された最大許可フレーム サイズを超え、有効な FCS 値を持つフレームの数。フレーム サイズには、FCS 値が含まれ、VLAN タグは含まれません。
System FCS error frames	インターフェイス上で受信された有効な長さ (バイト) を持ち、正常な FCS 値を持たないフレームの総数。
RxPortFifoFull drop frames	入力キューが満杯であるためドロップされた、インターフェイス上で受信されたフレームの総数。

1. FCS = Frame Check Sequence (フレーム チェック シーケンス)
2. MTU = Maximum Transmission Unit (最大伝送ユニット)

次の例では、特定のインターフェイスに対する **show controllers ethernet-controller phy** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller gigabitethernet0/2 phy
```

show controllers ethernet-controller

```
GigabitEthernet0/2 (gpn: 2, port-number: 2)
-----
=====
Port      Conf-Media  Active-Media  Attached
-----
Gi0/1    auto-select none          0 -Not Present
Gi0/2    auto-select none          0 -Not Present
=====
Other Information
-----
Port asic num      : 0
Port asic port num : 1
XCVR init completed : 0
Embedded PHY       : not present
SFP presence index : 0
SFP iter cnt       : 2564163d
SFP failed oper flag : 0x00000000
IIC error cnt      : 0
IIC error dsb cnt  : 0
IIC max sts cnt    : 0
Chk for link status : 1
Link Status        : 0
<テキスト出力は省略>
```

次の例では、**show controllers ethernet-controller port-asic configuration** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller port-asic configuration
=====
Switch 1, PortASIC 0 Registers
-----
DeviceType          : 000101BC
Reset               : 00000000
PmadMicConfig       : 00000001
PmadMicDiag         : 00000003
SupervisorReceiveFifoSramInfo : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo : 000001D0 000001D0 40000000
GlobalStatus        : 00000800
IndicationStatus    : 00000000
IndicationStatusMask : FFFFFFFF
InterruptStatus     : 00000000
InterruptStatusMask : 01FFE800
SupervisorDiag      : 00000000
SupervisorFrameSizeLimit : 000007C8
SupervisorBroadcast : 000A0F01
GeneralIO           : 000003F9 00000000 00000004
StackPcsInfo        : FFFF1000 860329BD 5555FFFF FFFFFFFF
                    FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo        : 73001630 00000003 7F001644 00000003
                    24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus  : 18E418E0
stackControlStatusMask : FFFFFFFF
TransmitBufferFreeListInfo : 00000854 00000800 0000FF8 00000000
                    0000088A 0000085D 0000FF8 00000000
TransmitRingFifoInfo : 00000016 00000016 40000000 00000000
                    0000000C 0000000C 40000000 00000000
TransmitBufferInfo  : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount : 00000F7A
TransmitBufferCommonCountPeak : 0000001E
TransmitBufferCommonCommonEmpty : 000000FF
NetworkActivity     : 00000000 00000000 00000000 02400000
DroppedStatistics   : 00000000
FrameLengthDeltaSelect : 00000001
SneakPortFifoInfo  : 00000000
```

```
MacInfo : 0EC0801C 00000001 0EC0801B 00000001
         00C0001D 00000001 00C0001E 00000001
```

<output truncated>

次の例では、**show controllers ethernet-controller port-asic statistics** コマンドの出力を示します。

```
Switch# show controllers ethernet-controller port-asic statistics
=====
Switch 1, PortASIC 0 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames          0 RxQ-0, wt-0 drop frames
4118966 RxQ-0, wt-1 enqueue frames          0 RxQ-0, wt-1 drop frames
      0 RxQ-0, wt-2 enqueue frames          0 RxQ-0, wt-2 drop frames

      0 RxQ-1, wt-0 enqueue frames          0 RxQ-1, wt-0 drop frames
    296 RxQ-1, wt-1 enqueue frames          0 RxQ-1, wt-1 drop frames
2836036 RxQ-1, wt-2 enqueue frames          0 RxQ-1, wt-2 drop frames

      0 RxQ-2, wt-0 enqueue frames          0 RxQ-2, wt-0 drop frames
      0 RxQ-2, wt-1 enqueue frames          0 RxQ-2, wt-1 drop frames
158377 RxQ-2, wt-2 enqueue frames          0 RxQ-2, wt-2 drop frames

      0 RxQ-3, wt-0 enqueue frames          0 RxQ-3, wt-0 drop frames
      0 RxQ-3, wt-1 enqueue frames          0 RxQ-3, wt-1 drop frames
      0 RxQ-3, wt-2 enqueue frames          0 RxQ-3, wt-2 drop frames

15 TxBufferFull Drop Count                 0 Rx Fcs Error Frames
  0 TxBufferFrameDesc BadCrc16             0 Rx Invalid Oversize Frames
  0 TxBuffer Bandwidth Drop Cou            0 Rx Invalid Too Large Frames
  0 TxQueue Bandwidth Drop Coun           0 Rx Invalid Too Large Frames
  0 TxQueue Missed Drop Statist            0 Rx Invalid Too Small Frames
74 RxBuffer Drop DestIndex Cou            0 Rx Too Old Frames
  0 SneakQueue Drop Count                 0 Tx Too Old Frames
  0 Learning Queue Overflow Fra           0 System Fcs Error Frames
  0 Learning Cam Skip Count

15 Sup Queue 0 Drop Frames                 0 Sup Queue 8 Drop Frames
  0 Sup Queue 1 Drop Frames               0 Sup Queue 9 Drop Frames
  0 Sup Queue 2 Drop Frames               0 Sup Queue 10 Drop Frames
  0 Sup Queue 3 Drop Frames               0 Sup Queue 11 Drop Frames
  0 Sup Queue 4 Drop Frames               0 Sup Queue 12 Drop Frames
  0 Sup Queue 5 Drop Frames               0 Sup Queue 13 Drop Frames
  0 Sup Queue 6 Drop Frames               0 Sup Queue 14 Drop Frames
  0 Sup Queue 7 Drop Frames               0 Sup Queue 15 Drop Frames
=====
Switch 1, PortASIC 1 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames          0 RxQ-0, wt-0 drop frames
    52 RxQ-0, wt-1 enqueue frames          0 RxQ-0, wt-1 drop frames
      0 RxQ-0, wt-2 enqueue frames          0 RxQ-0, wt-2 drop frames
```

<output truncated>

■ show controllers ethernet-controller

関連コマンド

コマンド	説明
show controllers cpu-interface	CPU ネットワーク ASIC の状態、および CPU に届くパケットの送受信の統計情報を表示します。
show controllers tcam	システム内のすべての Ternary CAM (TCAM) と CAM コントローラである TCAM インターフェイス ASIC のレジスタ ステートを表示します。

show controllers power inline

指定した Power over Ethernet (PoE) コントローラのレジスタの値を表示するには、**show controllers power inline** ユーザ EXEC コマンドを使用します。

```
show controllers power inline [instance] [| {begin | exclude | include} expression]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>instance</i>	(任意) 電源コントローラのインスタンス。各インスタンスは4つのポートに対応します。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。インスタンスを指定しない場合は、すべてのインスタンスが表示されます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

Catalyst 2960-24PC スイッチでは、指定できる *instance* の範囲は 0 ~ 1 です。0 と 1 以外のインスタンスの場合は、スイッチから出力が生成されません。

このコマンドは、すべてのスイッチで表示されますが、PoE スイッチのみで使用可能です。PoE をサポートしないスイッチの情報は提供されません。

このコマンドを使用すると、シスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ情報が表示されます。

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。

■ show controllers power inline

例

次の例では、Catalyst Catalyst 2960-24PC スイッチ上での **show controllers power inline** コマンドの出力を示します。

```
Switch> show controllers power inline
Alchemy instance 0, address 0
Pending event flag      :N N N N N N N N N N N N
Current State          :00 05 10 51 61 11
Current Event          :00 01 00 10 40 00
Timers                 :00 C5 57 03 12 20 04 B2 05 06 07 07
Error State            :00 00 00 00 10 00
Error Code              :00 00 00 00 00 00 00 00 00 00 00 00
Power Status           :N Y N N Y N N N N N N N
Auto Config            :N Y Y N Y Y Y Y Y Y Y Y
Disconnect             :N N N N N N N N N N N N
Detection Status       :00 00 00 30 00 00
Current Class          :00 00 00 30 00 00
Tweetie debug          :00 00 00 00
POE Commands pending at sub:
  Command 0 on each port :00 00 00 00 00 00
  Command 1 on each port :00 00 00 00 00 00
  Command 2 on each port :00 00 00 00 00 00
  Command 3 on each port :00 00 00 00 00 00
```

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
power inline	指定した PoE ポートまたはすべての PoE ポートの電力管理モードを設定します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの PoE ステータスを表示します。

show controllers tcam

システムのすべての Ternary CAM (TCAM)、および CAM コントローラである TCAM インターフェイス Application Specific Integrated Circuit (ASIC; 特定用途向け IC) のレジスタの状態を表示するには、**show controllers tcam** 特権 EXEC コマンドを使用します。

show controllers tcam [asic [number]] [detail] [| {begin | exclude | include} expression]

シンタックスの説明

asic	(任意) ポートの ASIC TCAM 情報を表示します。
number	(任意) 指定のポート ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 15 です。
detail	(任意) TCAM レジスタの詳細情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用することで、シスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立つ情報が表示されます。

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

次の例では、**show controllers tcam** コマンドの出力を示します。

```
Switch# show controllers tcam
```

```
-----  
TCAM-0 Registers  
-----
```

```
REV:      00B30103  
SIZE:     00080040  
ID:       00000000  
CCR:      00000000_F0000020  
  
RPID0:    00000000_00000000  
RPID1:    00000000_00000000  
RPID2:    00000000_00000000  
RPID3:    00000000_00000000
```

show controllers tcam

```

HRR0: 00000000_E000CAFC
HRR1: 00000000_00000000
HRR2: 00000000_00000000
HRR3: 00000000_00000000
HRR4: 00000000_00000000
HRR5: 00000000_00000000
HRR6: 00000000_00000000
HRR7: 00000000_00000000
<output truncated>

GMR31: FF_FFFFFFFF_FFFFFFFF
GMR32: FF_FFFFFFFF_FFFFFFFF
GMR33: FF_FFFFFFFF_FFFFFFFF

=====
TCAM related PortASIC 1 registers
=====
LookupType: 89A1C67D_24E35F00
LastCamIndex: 0000FFE0
LocalNoMatch: 000069E0
ForwardingRamBaseAddress:
                                00022A00 0002FE00 00040600 0002FE00 0000D400
                                00000000 003FBA00 00009000 00009000 00040600
                                00000000 00012800 00012900

```

関連コマンド

コマンド	説明
show controllers cpu-interface	CPU ネットワーク ASIC の状態、および CPU に届くパケットの送受信の統計情報を表示します。
show controllers ethernet-controller	ハードウェアまたはインターフェイスの内部レジスタから読み込まれる、各インターフェイスの送受信の統計情報を表示します。

show controllers utilization

スイッチまたは特定のポートの帯域利用率を表示するには、**show controllers utilization** ユーザ EXEC コマンドを使用します。

```
show controllers [interface-id] utilization [| {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) スイッチ インターフェイスの ID です。
begin	(任意) 指定した <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) 指定した <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例は、**show controllers utilization** コマンドの出力を示しています。

```
Switch> show controllers utilization
Port          Receive Utilization  Transmit Utilization
Fa0/1         0                    0
Fa0/2         0                    0
Fa0/3         0                    0
Fa0/4         0                    0
Fa0/5         0                    0
Fa0/6         0                    0
Fa0/7         0                    0
<output truncated>

<output truncated>

Switch Receive Bandwidth Percentage Utilization : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

■ show controllers utilization

次の例は、特定のポートでの **show controllers utilization** コマンドの出力を示します。

```
Switch> show controllers gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

表 2-24 show controllers utilization のフィールドの説明

フィールド	説明
Receive Bandwidth Percentage Utilization	スイッチの受信帯域利用率を表示します。これは、すべてのポートの受信トラフィックの合計をスイッチの受信容量で割ったものです。
Transmit Bandwidth Percentage Utilization	スイッチの送信帯域利用率を表示します。これは、すべてのポートの送信トラフィックの合計をスイッチの送信容量で割ったものです。
Fabric Percentage Utilization	スイッチの送信と受信の両方の帯域利用率の平均を表示します。

■ 関連コマンド

コマンド	説明
show controllers ethernet-controller	インターフェイスの内部レジスタを表示します。

show dot1x

スイッチ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、**show dot1x** ユーザ EXEC コマンドを使用します。

```
show dot1x [{all [summary] | interface interface-id} [details | statistics]] [| {begin |
exclude | include} expression]
```

シンタックスの説明

all [summary]	(任意) すべてのポートの IEEE 802.1x ステータスを表示します。
interface interface-id	(任意) 指定のポート (タイプ、モジュール、ポート番号を含む) の IEEE 802.1x のステータスを表示します。
details	(任意) IEEE 802.1x インターフェイスの詳細を表示します。
statistics	指定されたポートの IEEE 802.1x 統計情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	認証ステータスのマシン ステータスおよびポート ステータス フィールドに auth-fail-vlan が含まれるように表示が拡張されました。
12.2(25)SEE	コマンド構文が変更され、コマンド出力が修正されました。

使用上のガイドライン

ポートを指定しない場合は、グローバル パラメータおよびサマリーが表示されます。ポートを指定する場合、ポートの詳細が表示されます。

単一方向または双方向としてポート制御が設定され、この設定がスイッチの設定と対立する場合、**show dot1x {all | interface interface-id}** 特権 EXEC コマンド出力にその情報が表示されます。

ControlDirection = In (Inactive)

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 次の例では、**show dot1x** ユーザ EXEC コマンドの出力を示します。

```
Switch> show dot1x
Sysauthcontrol          Enabled
Dot1x Protocol Version      2
Critical Recovery Delay    100
Critical EAPOL            Disabled
```

次の例では、**show dot1x all** ユーザ EXEC コマンドの出力を示します。

```
Switch> show dot1x all
Sysauthcontrol          Enabled
Dot1x Protocol Version      2
Critical Recovery Delay    100
Critical EAPOL            Disabled

Dot1x Info for GigabitEthernet0/1
-----
PAE                      = AUTHENTICATOR
PortControl              = AUTO
ControlDirection        = Both
HostMode                 = SINGLE_HOST
Violation Mode          = PROTECT
ReAuthentication        = Disabled
QuietPeriod              = 60
ServerTimeout            = 30
SuppTimeout              = 30
ReAuthPeriod             = 3600 (Locally configured)
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30
RateLimitPeriod          = 0
```

<output truncated>

次の例では、**show dot1x all summary** ユーザ EXEC コマンドの出力を示します。

Interface	PAE	Client	Status
Gi0/1	AUTH	none	UNAUTHORIZED
Gi0/2	AUTH	00a0.c9b8.0072	AUTHORIZED
Gi0/3	AUTH	none	UNAUTHORIZED

次の例では、**show dot1x interface interface-id** ユーザ EXEC コマンドの出力を示します。

```
Switch> show dot1x interface gigabitethernet0/2
Dot1x Info for GigabitEthernet0/2
-----
PAE                      = AUTHENTICATOR
PortControl              = AUTO
ControlDirection        = In
HostMode                 = SINGLE_HOST
ReAuthentication        = Disabled
QuietPeriod              = 60
ServerTimeout            = 30
SuppTimeout              = 30
ReAuthPeriod             = 3600 (Locally configured)
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30
RateLimitPeriod          = 0
```


次の例では、**show dot1x interface interface-id details** ユーザ EXEC コマンドの出力を示します。

```
Switch# show dot1x interface gigabitethernet0/2 details
Dot1x Info for GigabitEthernet0/2
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

Dot1x Authenticator Client List Empty
```

次の例では、ポートがゲスト VLAN に割り当てられた状態でホスト モードが **multiple-hosts** モードに変更された場合の **show dot1x interface interface-id details** コマンドの出力を示します。

```
Switch# show dot1x interface gigabitethernet0/1 details
Dot1x Info for GigabitEthernet0/1
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Enabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
Guest-Vlan = 182

Dot1x Authenticator Client List Empty

Port Status = AUTHORIZED
Authorized By = Guest-Vlan
Operational HostMode = MULTI_HOST
Vlan Policy = 182
```

次の例では、**show dot1x interface interface-id statistics** コマンドの出力を示します。表 2-25 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show dot1x interface gigabitethernet0/2 statistics
Dot1x Authenticator Port Statistics for GigabitEthernet0/2
-----
RxStart = 0      RxLogoff = 0      RxResp = 1      RxRespID = 1
RxInvalid = 0    RxLenErr = 0      RxTotal = 2

TxReq = 2        TxReqID = 132    TxTotal = 134

RxVersion = 2    LastRxSrcMAC = 00a0.c9b8.0072
```

表 2-25 show dot1x statistics のフィールドの説明

フィールド	説明
RxStart	受信された有効な Extensible Authentication Protocol over LAN (EAPOL) -Start フレームの個数
RxLogoff	受信された EAPOL-Logoff フレームの数
RxResp	受信された有効な Extensible Authentication Protocol (EAP) -Response フレーム (Response/Identity フレーム以外) の個数
RxRespID	受信された EAP-Response/Identity フレームの数
RxInvalid	受信された EAPOL フレームのうち、フレーム タイプを認識できないフレームの数
RxLenError	受信された EAPOL フレームのうち、パケット本体の長さを示すフィールドが無効なフレームの数
RxTotal	受信されたすべてのタイプの有効な EAPOL フレームの数
TxReq	送信された EAP-Request フレーム (Request/Identity フレーム以外) の数
TxReqId	送信された EAP-Request/Identity フレームの個数
TxTotal	送信されたすべてのタイプの Extensible Authentication Protocol over LAN (EAPOL) フレームの個数
RxVersion	IEEE 802.1x バージョン 1 形式で受信されたパケットの数
LastRxSrcMac	最後に受信した EAPOL フレームで伝送された送信元 MAC (メディア アクセス 制御) アドレス

関連コマンド

コマンド	説明
dot1x default	IEEE 802.1x パラメータをデフォルト値に戻します。

show dtp

スイッチまたは指定されたインターフェイスのダイナミック トランッキング プロトコル (DTP) を表示するには、**show dtp** 特権 EXEC コマンドを使用します。

```
show dtp [interface interface-id] [| {begin | exclude | include} expression]
```

シンタックスの説明

interface <i>interface-id</i>	(任意) 指定されたインターフェイスのポート セキュリティ設定を表示します。有効なインターフェイスは物理ポート (タイプ、モジュール、ポート番号を含む) を含みます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show dtp** コマンドの出力を示します。

```
Switch# show dtp
Global DTP information
  Sending DTP Hello packets every 30 seconds
  Dynamic Trunk timeout is 300 seconds
  21 interfaces using DTP
```

次の例では、**show dtp interface** コマンドの出力を示します。

```
Switch# show dtp interface gigabitethernet0/1
DTP information for GigabitEthernet0/1:
TOS/TAS/TNS:                ACCESS/AUTO/ACCESS
TOT/TAT/TNT:                NATIVE/NEGOTIATE/NATIVE
Neighbor address 1:         000943A7D081
Neighbor address 2:         000000000000
Hello timer expiration (sec/state): 1/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state:                  S2:ACCESS
# times multi & trunk       0
Enabled:                    yes
In STP:                     no
```

■ show dtp

```
Statistics
-----
3160 packets received (3160 good)
0 packets dropped
    0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
6320 packets output (6320 good)
    3160 native
0 output errors
0 trunk timeouts
1 link ups, last link up on Mon Mar 01 1993, 01:02:29
0 link downs
```

関連コマンド

コマンド	説明
show interfaces trunk	インターフェイス トランク情報を表示します。

show eap

スイッチまたは特定のポートの Extensible Authentication Protocol (EAP) レジストレーション情報およびセッション情報を表示するには、**show eap** 特権 EXEC コマンドを使用します。

```
show eap {{registrations [method [name] | transport [name]]} | {sessions [credentials
name [interface interface-id] | interface interface-id | method name | transport
name]}} [credentials name | interface interface-id | transport name] [ | {begin |
exclude | include} expression]
```

シンタックスの説明

registrations	EAP レジストレーション情報を表示します。
method name	(任意) EAP 方式のレジストレーション情報を表示します。
transport name	(任意) EAP 伝送のレジストレーション情報を表示します。
sessions	EAP セッション情報を表示します。
credentials name	(任意) EAP 方式のレジストレーション情報を表示します。
interface interface-id	(任意) 指定のポート (タイプ、モジュール、ポート番号を含む) の EAP 情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

次のキーワードとともに **show eap registrations** 特権 EXEC コマンドを使用する場合、コマンド出力には次の情報が表示されます。

- None : EAP および登録された EAP 方式で使用されるすべての下位レベル
- **method name** キーワード : 登録された特定の方式
- **transport name** キーワード : 登録された特定の下のレベル

次のキーワードを含む **show eap sessions** 特権 EXEC コマンドを使用する場合、コマンド出力には次の情報が表示されます。

- None : すべてのアクティブな EAP セッション
- **credentials name** キーワード : 特定の証明書プロファイル
- **interface interface-id** キーワード : 特定のインターフェイスのパラメータ
- **method name** キーワード : 特定の EAP 方式
- **transport name** キーワード : 特定の下のレベル

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

次の例では、**show eap registrations** 特権 EXEC コマンドの出力を示します。

```
Switch> show eap registrations
```

```
Registered EAP Methods:
```

Method	Type	Name
4	Peer	MD5

```
Registered EAP Lower Layers:
```

Handle	Type	Name
2	Authenticator	Dot1x-Authenticator
1	Authenticator	MAB

次の例では、**show eap registrations transport** 特権 EXEC コマンドの出力を示します。

```
Switch> show eap registrations transport all
```

```
Registered EAP Lower Layers:
```

Handle	Type	Name
2	Authenticator	Dot1x-Authenticator
1	Authenticator	MAB

次の例では、**show eap sessions** 特権 EXEC コマンドの出力を示します。

```
Switch> show eap sessions
```

```
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticataInterface: Gi0/1
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
```

```
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticataInterface: Gi0/2
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0xA800000B Credentials profile: None
Lower layer context ID: 0x0D000005 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
```

```
<Output truncated>
```

次の例では、**show eap sessions interface *interface-id*** 特権 EXEC コマンドの出力を示します。

```
Switch# show eap sessions gigabitethernet0/1
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticataInterface: Gi0/1
Current method: None Method state: Uninitialised
Retransmission count: 1 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
```

関連コマンド

コマンド	説明
clear eap sessions	スイッチまたは特定のポートの EAP のセッション情報を表示します。

show energywise

EnergyWise の設定、エンティティのステータス、および Power over Ethernet (PoE) ポートのステータスを表示するには、**show energywise** 特権 EXEC コマンドを使用します。

```
show energywise neighbors [categories | children | domain | events | level [children |
current [children] | delta | delta children] | neighbors | recurrences | statistics | usage
[children] | version] [ | {begin | exclude | include} expression]
```

シンタックスの説明

categories	(任意) 電力レベルを表示します。
children	(任意) エンティティと PoE ポートのステータスを表示します。
domain	(任意) エンティティが属しているドメインを表示します。
events	(任意) ドメイン内の他のエンティティに送信されたイベント (メッセージ) のうちの最新の 10 件を表示します。
level [children current [children] delta delta children]	(任意) 使用可能な電力レベルを表示します。 <ul style="list-style-type: none"> • children : エンティティと PoE ポートの使用可能な電力レベル • current : エンティティの現在の電力レベル (任意) children : エンティティと PoE ポートの現在の電力レベル <ul style="list-style-type: none"> • delta : エンティティに関する現在の電力レベルと使用可能な電力レベルの差分 (任意) children : エンティティと PoE ポートに関する現在の電力レベルと使用可能な電力レベルの差分
neighbors	(任意) エンティティが属しているドメインのネイバー テーブルを表示します。
recurrence	(任意) EnergyWise での繰り返しの設定とステータスを表示します。
statistics	(任意) イベントのカウンタとエラーのカウンタを表示します。
usage [children]	(任意) エンティティの使用可能な電力を表示します。 <ul style="list-style-type: none"> • children : PoE ポートの使用可能な電力を表示します。
version	(任意) EnergyWise のバージョンを表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

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
Switch# show energywise
Interface  Role          Name          Usage      Lvl  Imp  Type
-----  -
Switch    lobby.1       558.0 (W)    10        1    parent

Switch# show energywise children
Interface  Role          Name          Usage      Lvl  Imp  Type
-----  -
Switch    lobby.1       558.0 (W)    10        1    parent
Gi0/1     interface    Gi0.1         0.0 (W)    1    1    child
Gi0/2     interface    Gi0.2         0.0 (W)    1    1    child
Gi0/3     interface    Gi0.3         0.0 (W)    1    1    child
Gi0/4     interface    Gi0.4         0.0 (W)    1    1    child
Gi0/5     interface    Gi0.5         0.0 (W)    1    1    child
Gi0/6     interface    Gi0.6         0.0 (W)    1    1    child
<output truncated>

Switch# show energywise domain
Name      : TG3560G-41
Domain    : cisco
Protocol  : udp
IP        : 2.2.2.21
Port      : 43440

Switch# show energywise events
-----
Sequence: 246818  References: 0:1  Errors:
Class:    PN_CLASS_QUERY
Action:   PN_ACTION_CPQR_POWERNET_QUERY_SET
Reply To: 8.8.8.24:43440
-----
Sequence: 246827  References: 0:1  Errors:
Class:    PN_CLASS_DISCOVERY
Action:   PN_ACTION_CPQR_POWERNET_DISCOVERY_DISCOVERY_UPDATE
Reply To: 8.8.8.24:43440
-----

Switch# show energywise level
Interface  Name          0      1      2      3      4      5      6      7      8      9      10
-----  -
lobby.1   0.0    558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0

Switch# show energywise level children
Interface  Name          0      1      2      3      4      5      6      7      8      9      10
-----  -
lobby.1   0.0    558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0  558.0
Gi0/1     Gi0.1        0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
Gi0/2     Gi0.2        0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
Gi0/3     Gi0.3        0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
Gi0/4     Gi0.4        0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
Gi0/5     Gi0.5        0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
<output truncated>

Switch# show energywise level current
Interface  Name          Level  Value
-----  -
lobby.1   10           558.0 (W)

Switch# show energywise level current children
Interface  Name          Level  Value
-----  -

```

show energywise

```

-----
lobby.1                10    558.0 (W)
Gi0/1                  Gi0.1    1    15.4 (W)
Gi0/2                  Gi0.2    1    15.4 (W)
Gi0/3                  Gi0.3    1    15.4 (W)
Gi0/4                  Gi0.4    1    15.4 (W)
Gi0/5                  Gi0.5    1    15.4 (W)
<output truncated>

```

Switch# show energywise level delta

```

                                     Levels (Watts)
Interface  Name          0      1      2      3      4      5      6      7      8      9      10
-----
lobby.1    lobby.1      -558.0  0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0

```

Switch# show energywise level delta child

```

                                     Levels (Watts)
Interface  Name          0      1      2      3      4      5      6      7      8      9      10
-----
lobby.1    lobby.1      -558.0  0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
Gi0/1      Gi0.1         0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
Gi0/2      Gi0.2         0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
Gi0/3      Gi0.3         0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
Gi0/4      Gi0.4         0.0    15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4   15.4
<output truncated>

```

Switch# show energywise neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

```

Id  Neighbor Name          Ip:Port          Prot  Capability
--  -----
1   Switch.A              2.2.2.29:43440  udp   S I
5   Switch.B              2.2.2.22:43440  udp   S I
7   Switch.C              2,2,2,33:43440  cdp   S I

```

Switch# show energywise recurrences

```

Id  Addr      Class Action Lvl Cron
--  ----
2   Gi0/17    QUERY SET      3 minutes: 0 hour: 8 day: * month: * weekday: *
3   Gi0/18    QUERY SET      3 minutes: 0 hour: 8 day: * month: * weekday: *
4   Gi0/19    QUERY SET      3 minutes: 0 hour: 8 day: * month: * weekday: *

```

Switch# show energywise statistics

Children: 48 Errors: 2 Drops: 0 Events: 14

Switch# show energywise usage

```

Interface  Name          Usage          Caliber
-----
lobby.1    lobby.1       558.0 (W)     max

```

```
Switch# show energywise usage child
Interface      Name      Usage      Caliber
-----
                lobby.1    558.0 (W)  max
Gi0/1          Gi0.1     0.0 (W)    presumed
Gi0/2          Gi0.2     0.0 (W)    presumed
Gi0/3          Gi0.3     0.0 (W)    presumed
Gi0/4          Gi0.4     0.0 (W)    presumed
Gi0/5          Gi0.5     0.0 (W)    presumed
<output truncated>
```

```
Switch# show energywise version
EnergyWise is Enabled
IOS Version: 12.2(50)SE
EnergyWise Specification: 1.0.1
```

関連コマンド

コマンド	説明
energywise (グローバル コンフィギュレーション)	エンティティ上で EnergyWise をイネーブルにして設定します。
energywise (インターフェイス コンフィギュレーション)	PoE ポート上で EnergyWise を設定します。

show env

スイッチのファン、温度、Redundant Power System (RPS; 冗長電源システム) の可用性、および電源情報を表示するには、**show env** ユーザ EXEC コマンドを使用します。

show env {**all** | **fan** | **power** | **rps**| **temperature**} [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

all	ファンと温度環境の両方の状態を表示します。
fan	スイッチ ファンの状態を表示します。
power	スイッチの電源の状態を表示します。
rps	RPS 300 がスイッチに接続されているかどうか表示します。
temperature	スイッチの温度ステータスを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show env all** コマンドの出力を示します。

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is AVAILABLE
```

次の例では、**show env fan** コマンドの出力を示します。

```
Switch> show env fan
FAN is OK
```

show errdisable detect

errdisable の検出状態を表示するには、**show errdisable detect** ユーザ EXEC コマンドを使用します。

show errdisable detect [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

表示された 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。

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

次の例では、**show errdisable detect** コマンドの出力を示します。

```
Switch> 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
lsgroup              Enabled     port
pagp-flap           Enabled     port
psecure-violation    Enabled     port/vlan
security-violatio    Enabled     port
sfp-config-mismat    Enabled     port
storm-control        Enabled     port
udld                 Enabled     port
vmps                 Enabled     port
```

関連コマンド

コマンド	説明
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します。
show errdisable flap-values	認識されている状態のエラー情報を表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

show errdisable flap-values

ある原因をエラーとして認識させる条件を表示するには、**show errdisable flap-values** ユーザ EXEC コマンドを使用します。

show errdisable flap-values [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

Flaps 列では、指定のインターバル以内にステートへの変更を何回行くと、エラーが検出されてポートがディセーブルになるのかを表示します。たとえば、3 つの Dynamic Trunking Protocol (DTP) ステート (ポート モード アクセス/トランク)、またはポート集約プロトコル (PAgP) フラップが 30 秒間隔で変更された場合、または 5 つのリンク ステート (リンク アップ/ダウン) が 10 秒間隔で変更された場合は、エラーと見なされてポートがシャットダウンします。

ErrDisable Reason	Flaps	Time (sec)
pagp-flap	3	30
dtp-flap	3	30
link-flap	5	10

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

次の例では、**show errdisable flap-values** コマンドの出力を示します。

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----
pagp-flap            3         30
dtp-flap              3         30
link-flap             5         10
```

■ show errdisable flap-values

関連コマンド

コマンド	説明
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	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

show errdisable recovery

errdisable 回復タイマー情報を表示するには、**show errdisable recovery** ユーザ EXEC コマンドを使用します。

show errdisable recovery [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

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

次の例では、**show errdisable recovery** コマンドの出力を示します。

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----
udld                  Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
loopback             Disabled
```

■ show errdisable recovery

```

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
-----
Gi0/2          link-flap                279

```



(注)

unicast-flood フィールドは出力に表示されますが、無効になっています。

関連コマンド

コマンド	説明
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 flap-values	認識されている状態のエラー情報を表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

show etherchannel

チャンネルの EtherChannel 情報を表示するには、**show etherchannel** ユーザ EXEC 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} [ |
{begin | exclude | include} expression]
```

シンタックスの説明

<i>channel-group-number</i>	(任意) チャンネル グループの番号です。指定できる範囲は 1 ~ 6 です。
detail	EtherChannel の詳細を表示します。
load-balance	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	EtherChannel ポート情報を表示します。
port-channel	ポートチャンネル情報を表示します。
protocol	EtherChannel で使用されるプロトコルを表示します。
summary	各チャンネル グループのサマリーを 1 行で表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

channel-group 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。

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 次の例では、**show etherchannel 1 detail** コマンドの出力を示します。

```
Switch> 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: Gi0/1
-----

Port state      = Up Mstr In-Bndl
Channel group = 1           Mode = Active           Gchange = -
Port-channel = Po1         GC = -             Pseudo port-channel = Po1
Port index      = 0         Load = 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
Gi0/1    SA     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   Gi0/1     Active        0
  0     00   Gi0/2     Active        0

Time since last port bundled: 01d:20h:20m:20s   Gi0/2
```

次の例では、**show etherchannel 1 summary** コマンドの出力を示します。

```
Switch> 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        Gi0/1(P)   Gi0/2(P)
```

次の例では、**show etherchannel 1 port-channel** コマンドの出力を示します。

```
Switch> 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
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    Gi0/1     Active        0
      0    00    Gi0/2     Active        0

Time since last port bundled:  01d:20h:24m:44s   Gi0/2
```

次の例では、**show etherchannel protocol** コマンドの出力を示します。

```
Switch# show etherchannel protocol
          Channel-group listing:
          -----
Group: 1
-----
Protocol: LACP

Group: 2
-----
Protocol: PAgP
```

関連コマンド

コマンド	説明
channel-group	EtherChannel グループにイーサネット ポートを割り当てます。
channel-protocol	チャネリングを管理するため、ポート上で使用されるプロトコルを制限します。
interface port-channel	ポート チャネルへのアクセスや、ポート チャネルの作成を行います。

show fallback profile

スイッチに設定されたフォールバック プロファイルを表示するには、**show fallback profile** 特権 EXEC コマンドを使用します。

show fallback profile [**append** | **begin** | **exclude** | **include** | { [**redirect** | **tee**] *url* } *expression*]

シンタックスの説明

append	(任意) 指定 URL にリダイレクト出力を付加します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
redirect	(任意) 指定 URL に出力をコピーします。
tee	(任意) 指定 URL に出力をコピーします。
<i>expression</i>	参照ポイントとして使用する出力内の式です。
<i>url</i>	出力を誘導する URL。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチで設定されたプロファイルを表示するには、**show fallback profile** 特権 EXEC コマンドを使用します。

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

次の例では、**show fallback profile** コマンドの出力を示します。

```
switch# show fallback profile
Profile Name: dot1x-www
-----
Description          : NONE
IP Admission Rule    : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-----
Description          : NONE
IP Admission Rule    : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-----
Description          : NONE
IP Admission Rule    : NONE
IP Access-Group IN: NONE
```

関連コマンド

コマンド	説明
dot1x fallback profile	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メカニズムとして Web 認証を使用するようポートを設定します。
fallback profile 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 rule	スイッチ ポートで Web 認証をイネーブルにします。
ip admission name proxy http	スイッチで Web 認証をグローバルにイネーブルにします。
show dot1x [interface <i>interface-id</i>]	指定されたポートの IEEE 802.1x の状態を表示します。

show flowcontrol

フロー制御ステータスおよび統計情報を表示するには、**show flowcontrol** ユーザ EXEC コマンドを使用します。

```
show flowcontrol [interface interface-id | module number] [ | {begin | exclude | include}
expression]
```

シンタックスの説明

interface interface-id	(任意) 特定のインターフェイスのフロー制御ステータスおよび統計情報を表示します。
module number	(任意) すべてのスイッチ上のインターフェイスのフロー制御ステータスと統計情報を表示します。有効なモジュール番号は 1 のみです。このオプションは、特定のインターフェイス ID を入力した場合に使用できなくなります。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定のインターフェイスのフロー制御ステータスおよび統計情報を表示するには、このコマンドを使用します。

スイッチ インターフェイス情報をすべて表示するには、**show flowcontrol** コマンドを使用します。**show flowcontrol** コマンドの出力は、**show flowcontrol module number** コマンドの出力と同じになります。

特定のインターフェイスの情報を表示するには、**show flowcontrol interface interface-id** コマンドを使用します。

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

次の例では、**show flowcontrol** コマンドの出力を示します。

```
Switch> show flowcontrol
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
          admin    oper    admin    oper
-----
Gi0/1     Unsupp.  Unsupp.  off      off      0        0
Gi0/2     desired  off      off      off      0        0
Gi0/3     desired  off      off      off      0        0
<output truncated>
```


次の例では、**show flowcontrol interface interface-id** コマンドの出力を示します。

```
Switch> show flowcontrol gigabitethernet0/2
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
-----
-----
-----
Gi0/2        desired off      off      off      0      0
```

関連コマンド

コマンド	説明
flowcontrol	インターフェイスの受信フロー制御ステータスを設定します。

show interfaces

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管理ステータスおよび動作ステータスを表示するには、**show interfaces** 特権 EXEC コマンドを使用します。

```
show interfaces [interface-id | vlan vlan-id] [accounting | capabilities [module number] |
counters | description | etherchannel | flowcontrol | pruning | stats | status
[err-disabled] | switchport [backup | module number] | transceiver properties |
detail [module number] | trunk] [ | {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) 有効なインターフェイスは、物理ポート (タイプ、モジュール、およびポート番号を含む) やポート チャネルなどです。ポート チャネル範囲は 1 ~ 6 です。
<i>vlan</i> <i>vlan-id</i>	(任意) VLAN ID です。指定できる範囲は 1 ~ 4094 です。
accounting	(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 packets、オクテットを含む) を表示します。 (注) ソフトウェアで処理された packets のみが表示されます。ハードウェアでスイッチングされる packets は表示されません。
capabilities	(任意) すべてのインターフェイスまたは指定の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、VLAN ID に使用できません。
<i>module number</i>	(任意) スイッチ上のすべてのインターフェイスの機能、スイッチポート コンフィギュレーション、またはトランシーバ特性 (上記のキーワードに対応) を表示します。有効なモジュール番号は 1 のみです。このオプションは、特定のインターフェイス ID を入力するときは利用できません。
counters	(任意) show interfaces counters コマンドを参照してください。
description	(任意) 特定の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。
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。
pruning	(任意) インターフェイス 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スイッチング パスによる入出力 packets 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 <i>unsupported</i> 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。
switchport	(任意) ポート ロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
backup	(任意) スイッチ上の指定したインターフェイスまたはすべてのインターフェイスの Flex Link バックアップ インターフェイス コンフィギュレーションとステータスを表示します。

transceiver [detail properties]	(任意) 低密度波長分割多重 (CWDM) ¹ または高密度波長分割多重 (DWDM) ² SFP モジュール インターフェイスの物理プロパティを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • detail : (任意) 高低の番号、アラーム情報を含む較正プロパティを表示します。 • properties : (任意) インターフェイスの速度とデュプレックスの設定を表示します。
trunk	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ッキング ポートの情報のみが表示されます。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

1. Coarse Wavelength Division Multiplexing (CWDM; 低密度波長分割多重)
2. Dense Wavelength Division Multiplexing (DWDM; 高密度波長分割多重)



(注)

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tring に表示されますが、サポートされていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	backup 、 counters 、 detail 、および trunk キーワードが追加されました。
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

- スイッチ上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 module 1** を使用します。これ以外の番号の入力は無効です。
- 特定の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。
- スイッチ上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)。
- 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 interfaces switchport module 1** を使用します。これ以外の番号の入力は無効です。

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

次の例では、インターフェイスに対する **show interface** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/2
GigabitEthernet0/2 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never
  Last clearing of "show interfaces" counters never
  Input queue: 0/75/0/0 (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
    2 packets input, 1040 bytes, 0 no buffer
  Received 0 broadcasts, 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
  4 packets output, 1040 bytes, 0 underruns
  0 output errors, 0 collisions, 3 interface resets
  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
```

次の例では、**show interfaces accounting** コマンドの出力を示します。

```
Switch# show interfaces accounting
Vlan1
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
          IP           1094395   131900022  559555     84077157
          Spanning Tree 283896   17033760   42         2520
          ARP           63738    3825680    231        13860

Interface Vlan2 is disabled
Vlan7
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
Vlan31
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

GigabitEthernet0/1
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
          Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
```

<output truncated>

次の例では、インターフェイスに対する **show interfaces capabilities** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet0/2 capabilities
GigabitEthernet0/2
  Model:                WS-C2960G-24TC-L
  Type:                 10/100/1000BaseTX
  Speed:                10,100,1000,auto
  Duplex:               full,auto
  Trunk encap.type:     802.1Q
  Trunk mode:           on,off,desirable,nonegotiate
```

```

Channel:                yes
Broadcast suppression: percentage(0-100)
Flowcontrol:            rx-(off,on,desired),tx-(none)
Fast Start:             yes
QoS scheduling:         rx-(not configurable on per port basis),tx-(4q2t)
CoS rewrite:            yes
ToS rewrite:            yes
UDLD:                   yes
Inline power:           no
SPAN:                   source/destination
PortSecure:             yes
Dot1x:                  yes
Multiple Media Types:   rj45, sfp, auto-select

```

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。

```

Switch# show interfaces gigabitethernet0/2 description
Interface Status          Protocol Description
Gi0/2          up              down        Connects to Marketing

```

次の例では、スイッチにポート チャンネルが設定されている場合の **show interfaces etherchannel** コマンドの出力を示します。

```

Switch# show interfaces etherchannel
-----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/1          Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/2          Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port        = 10/3          Number of ports = 0
GC                        = 0x00000000    HotStandBy port = null
Port state                = Port-channel Ag-Not-Inuse

```

次の例では、VTP ドメイン内でプルーンングがイネーブルになっている場合の **show interfaces interface-id pruning** コマンドの出力を示します。

```

Switch# show interfaces gigabitethernet0/2 pruning
Port   Vlans pruned for lack of request by neighbor
Gi0/2   3,4

Port   Vlans traffic requested of neighbor
Gi0/2   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。

```

Switch# 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

```

次の例では、**show interfaces status** コマンドの出力の一部を示します。すべてのインターフェイスのステータスが表示されます。

```
Switch# show interfaces status
Port      Name          Status      Vlan      Duplex  Speed Type
Gi0/1     Gi0/1         notconnect  1         auto    auto 10/100/1000BaseTX
Gi0/2     Gi0/2         notconnect  1         auto    auto 10/100/1000BaseTX
Gi0/3     Gi0/3         notconnect  1         auto    auto 10/100/1000BaseTX
Gi0/4     Gi0/4         notconnect  1         auto    auto 10/100/1000BaseTX
Gi0/5     Gi0/5         notconnect  1         auto    auto 10/100/1000BaseTX
Gi0/6     Gi0/6         notconnect  1         auto    auto 10/100/1000BaseTX
```

<テキスト出力は省略>

次の例では、**show interfaces status err-disabled** コマンドの出力を示します。errdisable ステートのインターフェイスのステータスを表示します。

```
Switch# show interfaces status err-disabled
Port      Name          Status      Reason
Gi0/2     Gi0/2         err-disabled dtp-flap
```

次の例では、ポートに対する **show interfaces switchport** コマンドの出力を示します。表 2-26 に、この出力で表示されるフィールドの説明を示します。



(注)

プライベート VLAN はこのリリースではサポートされないため、フィールドは適用されません。

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association:10 (VLAN0010) 502 (VLAN0502)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

表 2-26 show interfaces switchport のフィールドの説明

フィールド	説明
Name	ポートの名前を表示します。
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ー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	プルーニングに適切な 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ーネーブルになっているか (True) ディセーブルになっているか (False) 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 がイーネーブルである VLAN ID を表示します。
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。

次の例では、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
  Active Interface    Backup Interface    State
  -----
  Fa0/1              Fa0/2              Active Up/Backup Standby
  Fa0/3              Fa0/5              Active Down/Backup Up
  Po1                Po2                Active Standby/Backup Up
```

次の例では、**show interfaces switchport backup** コマンドの出力を示します。この例では、スイッチで VLAN 1 ~ 50、60、100 ~ 120 が設定されています。

```
Switch(config)#interface gigabitEthernet 0/6
Switch(config-if)#switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、Gi0/8 が VLAN 60 および VLAN 100 ~ 120 のトラフィックを転送し、Gi0/6 が VLAN 1 ~ 50 のトラフィックを転送します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

```
Vlans on Interface Gi 0/6: 1-50
Vlans on Interface Gi 0/8: 60, 100-120
```

Flex Link インターフェイスがダウンすると (LINK_DOWN)、このインターフェイスで優先される VLAN は Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi0/6 がダウンすると、Gi0/8 が Flex Link ペアのすべての VLAN を伝送します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

```
Vlans on Interface Gi 0/6:
Vlans on Interface Gi 0/8: 1-50, 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi0/6 がアップになって、このインターフェイスに指定されていた VLAN がピア インターフェイス Gi0/8 上でブロックされ、Gi0/6 に転送されます。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

```
Vlans on Interface Gi 0/6: 1-50
Vlans on Interface Gi 0/8: 60, 100-120
```

次の例では、**show interfaces interface-id pruning** コマンドの出力を示します。

```
Switch# show interfaces gigabitEthernet0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

次の例では、**show interfaces interface-id trunk** コマンドの出力を示します。ポートのトランキング情報が表示されます。

```
Switch# show interfaces gigabitEthernet0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi0/1     auto      negotiate      trunking    1

Port      Vlans allowed on trunk
Gi0/1     1-4094
```



```

Port          Vlans allowed and active in management domain
Gi0/1         1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi0/1         1-4

```

次の例では、**show interfaces interface-id transceiver properties** コマンドの出力を示します。

```

Switch# show interfaces gigabitethernet0/1 transceiver properties
Name : Gi0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: N/A
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
Configured Media: sfp
Active Media: sfp
Attached: 10/100/1000BaseTX SFP-10/100/1000BaseTX

```

次の例では、**show interfaces interface-id transceiver detail** コマンドの出力を示します。

```

Switch# show interfaces gigabitethernet0/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally 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)
Gi0/3	41.5	110.0	103.0	-8.0	-12.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi0/3	3.20	4.00	3.70	3.00	2.95

Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi0/3	31.0	84.0	70.0	4.0	2.0

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi0/3	-0.0 (-0.0)	-0.0	-0.0	-0.0	-0.0

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi0/3	N/A (-0.0) --	-0.0	-0.0	-0.0	-0.0

関連コマンド

コマンド	説明
switchport access	ポートをスタティック アクセス ポートまたはダイナミック アクセス ポートとして設定します。
switchport block	インターフェイス上で未知のユニキャスト、または未知のマルチキャスト トラフィックをブロックします。
switchport backup interface	相互バックアップを提供するレイヤ 2 インターフェイスのペアである Flex Link を設定します。
switchport mode	ポートの VLAN メンバシップ モードを設定します。
switchport protected	同じスイッチの他の保護されたポートからレイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離します。
switchport trunk pruning	トランキング モードのポートの VLAN プルーニング適格リストを設定します。

show interfaces counters

スイッチまたは指定されたインターフェイスの各カウンタを表示するには、**show interfaces counters** 特権 EXEC コマンドを使用します。

```
show interfaces [interface-id | vlan vlan-id] counters [errors | etherchannel | protocol status | trunk] [ | {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) 物理インターフェイスの ID (タイプ、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。
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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注)

vlan vlan-id キーワードは、コマンドラインのヘルプ スtringには表示されますが、サポートされていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

キーワードを指定しない場合は、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。

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。

■ show interfaces counters

例

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。

```
Switch# show interfaces counters
Port           InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi0/1          0           0            0            0
Gi0/2          0           0            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。

```
Switch# 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
FastEthernet0/1: Other, IP, ARP, CDP
FastEthernet0/2: Other, IP
FastEthernet0/3: Other, IP
FastEthernet0/4: Other, IP
FastEthernet0/5: Other, IP
FastEthernet0/6: Other, IP
FastEthernet0/7: Other, IP
FastEthernet0/8: Other, IP
FastEthernet0/9: Other, IP
FastEthernet0/10: Other, IP, CDP
```

<output truncated>

次の例では、**show interfaces counters trunk** コマンドの出力を示します。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。

```
Switch# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1         0              0              0
Gi0/2         0              0              0
Gi0/3         80678         4155           0
Gi0/4         82320         126            0
Gi0/5         0              0              0
```

<output truncated>

関連コマンド

コマンド	説明
show interfaces	追加のインターフェイスの特性を表示します。

show inventory

ハードウェアの Product Identification (PID; 製品識別) 情報を表示するには、**show inventory** ユーザ EXEC コマンドを使用します。

show inventory [*entity-name* | **raw**] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>entity-name</i>	(任意) 指定のエンティティを表示します。たとえば、Small Form-factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュールが取り付けられているインターフェイス (gigabitethernet0/1 など) を入力します。
raw	(任意) デバイスのすべてのエンティティを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

コマンドでは大文字と小文字が区別されます。引数がない場合、**show inventory** コマンドは製品識別情報を持つすべての識別可能なエンティティのコンパクト ダンプを生成します。コンパクト ダンプには、エンティティの場所 (スロット ID)、エンティティの説明、およびそのエンティティの Unique Device Identifier (UDI) (PID、VID、および SN) が表示されます。



(注)

PID がない場合は、**show inventory** コマンドを入力しても出力は表示されません。

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

次の例では、**show inventory** コマンドの出力を示します。

```
Switch> show inventory
NAME: "1", DESCR: "WS-C2960-48TC-L"
PID: WS-C2960-24TC-L , VID: 02 , SN: FHH0923D075

NAME: "GigabitEthernet0/1", DESCR: "100BaseBX-10D SFP"
PID: , VID: , SN: NEC09050251

NAME: "GigabitEthernet0/2", DESCR: "100BaseBX-10U SFP"
PID: , VID: , SN: NEC09050020
```

show ip arp inspection

ダイナミック アドレス解決プロトコル (ARP) インスペクションの設定と動作ステータスを表示したり、すべての VLAN または指定したインターフェイス/VLAN に関してダイナミック ARP インスペクションのステータスを表示したりするには、**show ip arp inspection** 特権 EXEC コマンドを使用します。

```
show ip arp inspection [interfaces [interface-id] | log | statistics [vlan vlan-range] | vlan
vlan-range] [| {begin | exclude | include} expression]
```

シンタックスの説明

interfaces [<i>interface-id</i>]	(任意) 指定したインターフェイスまたはすべてのインターフェイスに関して ARP パケットの信頼状態とレート制限を表示します。有効なインターフェイスは、物理ポートおよびポート チャネルです。
log	(任意) ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。
statistics [vlan <i>vlan-range</i>]	(任意) 指定した VLAN に関して転送されたパケット、廃棄されたパケット、MAC 検証で不合格となったパケット、IP 検証で不合格となったパケット、アクセス コントロール リスト (ACL) で許可および拒否されたパケット、および DHCP で許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合や範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブル (アクティブ) になっている VLAN に関してのみ情報が表示されます。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
vlan <i>vlan-range</i>	(任意) 指定した VLAN に関してダイナミック ARP インスペクションの設定と動作ステータスを表示します。VLAN が指定されていない場合や範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブル (アクティブ) になっている VLAN に関してのみ情報が表示されます。 VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

show ip arp inspection

使用上のガイドライン

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 次の例では、**show ip arp inspection** コマンドの出力を示します。

```
Switch# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

Vlan      Configuration      Operation      ACL Match      Static ACL
-----
1         Enabled            Active        deny-all      No

Vlan      ACL Logging      DHCP Logging      Probe Logging
-----
1         Acl-Match        All            Permit

Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
-----
1         0              0            0              0

Vlan      DHCP Permits      ACL Permits      Probe Permits      Source MAC Failures
-----
1         0              0            0              0

Vlan      Dest MAC Failures      IP Validation Failures      Invalid Protocol Data
-----
1         0              0              0
```

次の例では、**show ip arp inspection interfaces** コマンドの出力を示します。

```
Switch# show ip arp inspection interfaces

Interface      Trust State      Rate (pps)      Burst Interval
-----
Gi0/1          Untrusted        15              1
Gi0/2          Untrusted        15              1
Gi0/3          Untrusted        15              1
```

次の例では、**show ip arp inspection interfaces interface-id** コマンドの出力を示します。

```
Switch# show ip arp inspection interfaces gigabitethernet0/1

Interface      Trust State      Rate (pps)      Burst Interval
-----
Gi0/1          Untrusted        15              1
```

次の例では、**show ip arp inspection log** コマンドの出力を示します。ここでは、クリアされる前のログバッファの内容が表示されます。

```
Switch# show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 10 entries per 300 seconds.

Interface      Vlan      Sender MAC      Sender IP      Num Pkts      Reason      Time
-----
Gi0/1          5         0003.0000.d673  192.2.10.4    5             DHCP Deny   19:39:01 UTC
Mon Mar 1 1993
Gi0/1          5         0001.0000.d774  128.1.9.25    6             DHCP Deny   19:39:02 UTC
Mon Mar 1 1993
Gi0/1          5         0001.c940.1111  10.10.10.1    7             DHCP Deny   19:39:03 UTC
Mon Mar 1 1993
```



```

Gi0/1      5      0001.c940.1112  10.10.10.2      8  DHCP Deny      19:39:04 UTC
Mon Mar 1 1993
Gi0/1      5      0001.c940.1114  173.1.1.1       10 DHCP Deny      19:39:06 UTC
Mon Mar 1 1993
Gi0/1      5      0001.c940.1115  173.1.1.2       11 DHCP Deny      19:39:07 UTC
Mon Mar 1 1993
Gi0/1      5      0001.c940.1116  173.1.1.3       12 DHCP Deny      19:39:08 UTC
Mon Mar 1 1993

```

ログバッファのオーバーフローが発生すると、ログイベントがログバッファと整合しなくなり、**show ip arp inspection log** 特権 EXEC コマンドの出力表示に影響が及びます。出力表示で、パケット数と時刻を除くすべてのデータが -- と表示されます。このエントリに関してそれ以外の統計情報は表示されません。このエントリに関する情報が表示されるようにするには、**ip arp inspection log-buffer** 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、ログバッファ内のエントリの数を増やすか、またはロギング レートを高めます。

次の例では、**show ip arp inspection statistics** コマンドの出力を示します。ここでは、すべてのアクティブ VLAN に関してダイナミック ARP インспекションで処理されたパケットの統計情報が表示されます。

```

Switch# show ip arp inspection statistics
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
5          3              4618         4605            4
2000      0              0            0               0

Vlan      DHCP Permits    ACL Permits    Source MAC Failures
----      -
5          0              12            0
2000      0              0             0

Vlan      Dest MAC Failures  IP Validation Failures
----      -
5          0                 9
2000      0                 0

```

show ip arp inspection statistics コマンドの場合、スイッチは信頼できるダイナミック ARP インспекション ポート上の ARP 要求と ARP 応答ごとに、転送されたパケットの数を増分します。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増分し、適切な失敗数を増分します。

次の例では、**show ip arp inspection statistics vlan 5** コマンドの出力を示します。ここでは、VLAN 5 に関してダイナミック ARP インспекションで処理されたパケットの統計情報が表示されます。

```

Switch# show ip arp inspection statistics vlan 5
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
5          3              4618         4605            4

Vlan      DHCP Permits    ACL Permits    Source MAC Failures
----      -
5          0              12            0

Vlan      Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
----      -
5          0                 9                      3

```

■ show ip arp inspection

次の例では、**show ip arp inspection vlan 5** コマンドの出力を示します。ここでは、VLAN 5 に関してダイナミック ARP インспекションの設定と動作ステータが表示されます。

```
Switch# show ip arp inspection vlan 5
Source Mac Validation      :Enabled
Destination Mac Validation :Enabled
IP Address Validation      :Enabled

Vlan      Configuration      Operation      ACL Match      Static ACL
----      -
5         Enabled              Active        second         No

Vlan      ACL Logging              DHCP Logging
----      -
5         Acl-Match                All
```

■ 関連コマンド

コマンド	説明
arp access-list	ARP ACL を定義します。
clear ip arp inspection log	ダイナミック ARP インспекションのログ バッファをクリアします。
clear ip arp inspection statistics	ダイナミック ARP インспекションの統計情報をクリアします。
ip arp inspection log-buffer	ダイナミック ARP インспекションのログ バッファを設定します。
ip arp inspection vlan logging	VLAN ごとにロギングされるパケットのタイプを制御します。
show arp access-list	ARP アクセス リストの詳細を表示します。

show ip dhcp snooping

DHCP スヌーピング設定を表示するには、**show ip dhcp snooping** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping [| {**begin** | **exclude** | **include**} *expression*]



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show ip dhcp snooping** コマンドの出力を示します。

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
GigabitEthernet0/1      yes         unlimited
GigabitEthernet0/2      yes         unlimited
```

関連コマンド

コマンド	説明
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。

show ip dhcp snooping binding

スイッチ上にあるすべてのインターフェイスの DHCP スヌーピング バインディング データベースと設定情報を表示するには、**show ip dhcp snooping binding** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>ip-address</i>	(任意) バインディング エントリ IP アドレスを指定します。
<i>mac-address</i>	(任意) バインディング エントリ MAC (メディアアクセス制御) アドレスを指定します。
interface <i>interface-id</i>	(任意) バインディング入力インターフェイスを指定します。
vlan <i>vlan-id</i>	(任意) バインディング エントリ VLAN を指定します。
begin	<i>expression</i> と一致する行から表示を開始します。
exclude	<i>expression</i> と一致する行を表示から除外します。
include	指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

show ip dhcp snooping binding コマンドの出力は、ダイナミックに設定されたバインディングだけを表示します。DHCP スヌーピング バインディング データベース内のダイナミックおよびスタティックに設定されたバインディングを表示するには、**show ip source binding** 特権 EXEC コマンドを使用します。

DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

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

次の例では、スイッチの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding
MacAddress          IpAddress          Lease(sec)  Type             VLAN  Interface
-----
01:02:03:04:05:06  10.1.2.150         9837        dhcp-snooping   20    GigabitEthernet0/1
00:D0:B7:1B:35:DE  10.1.2.151         237         dhcp-snooping   20    GigabitEthernet0/2
Total number of bindings: 2
```

次の例では、特定の IP アドレスの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding 10.1.2.150
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9810          dhcp-snooping  20     GigabitEthernet0/1
Total number of bindings: 1
```

次の例では、特定の MAC アドレスの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding 0102.0304.0506
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9788          dhcp-snooping  20     GigabitEthernet0/2
Total number of bindings: 1
```

次の例では、ポートの DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding interface gigabitethernet0/2
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN    Interface
-----
00:30:94:C2:EF:35  10.1.2.151    290           dhcp-snooping  20     GigabitEthernet0/2
Total number of bindings: 1
```

次の例では、VLAN 20 の DHCP スヌーピング バインディング エントリを表示する方法を示します。

```
Switch> show ip dhcp snooping binding vlan 20
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9747          dhcp-snooping  20     GigabitEthernet0/1
00:00:00:00:00:02  10.1.2.151    65            dhcp-snooping  20     GigabitEthernet0/2
Total number of bindings: 2
```

表 2-27 に、show ip dhcp snooping binding コマンドの出力に表示される各フィールドの説明を示します。

表 2-27 show ip dhcp snooping binding コマンド出力

フィールド	説明
MacAddress	クライアント ハードウェアの MAC アドレス
IpAddress	DHCP サーバに割り当てられたクライアント IP アドレス
Lease(sec)	IP アドレスに対する残りのリース時間
Type	バインディング タイプ
VLAN	クライアント インターフェイスの VLAN 番号
Interface	DHCP クライアント ホストに接続するインターフェイス
Total number of bindings	スイッチに設定される合計バインディング数 (注) コマンド出力では、合計バインディング数が表示されないこともあります。たとえば、200 バインディングがスイッチに設定されてすべてのバインディングが表示される前に表示を停止させた場合、合計数は変更されません。

■ show ip dhcp snooping binding

関連コマンド

コマンド	説明
ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。

show ip dhcp snooping database

DHCP スヌーピング バインディング データベース エージェントのステータスを表示するには、**show ip dhcp snooping database** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping database [detail] [| {begin | exclude | include} expression]



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

detail	(任意) 詳細なステータスと統計情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、**show ip dhcp snooping database** コマンドの出力を示します。

```
Switch> show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :          0   Startup Failures :          0
Successful Transfers :          0   Failed Transfers :          0
Successful Reads    :          0   Failed Reads     :          0
Successful Writes   :          0   Failed Writes    :          0
Media Failures      :          0
```

■ show ip dhcp snooping database

次の例では、**show ip dhcp snooping database detail** コマンドの出力を示します。

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts      :      21   Startup Failures :      0
Successful Transfers :      0   Failed Transfers :     21
Successful Reads    :      0   Failed Reads     :      0
Successful Writes   :      0   Failed Writes    :     21
Media Failures      :      0

First successful access: Read

Last ignored bindings counters :
Binding Collisions   :      0   Expired leases   :      0
Invalid interfaces  :      0   Unsupported vlans :      0
Parse failures       :      0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions   :      0   Expired leases   :      0
Invalid interfaces  :      0   Unsupported vlans :      0
Parse failures       :      0
```

関連コマンド

コマンド	説明
ip dhcp snooping	VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping database	DHCP スヌーピング バインディング データベース エージェントまたはバインディング ファイルを設定します。
show ip dhcp snooping	DHCP スヌーピング情報を表示します。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報をサマリー形式または詳細形式で表示するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping statistics [detail] [| {begin | exclude | include} expression]



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

detail	(任意) 詳細な統計情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(37)SE	このコマンドが追加されました。

使用上のガイドライン

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。

スイッチ スタックでは、すべての統計情報がスタック マスター上に生成されます。新しいスタック マスターを選択すると、統計カウンタがリセットされます。

例

次の例では、**show ip dhcp snooping statistics** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics
Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

次の例では、**show ip dhcp snooping statistics detail** コマンドの出力を示します。

```
Switch> 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
```

show ip dhcp snooping statistics

```

Interface Down = 0
Unknown output interface = 0
Reply output port equal to input port = 0
Packet denied by platform = 0

```

表 2-28 に、DHCP スヌーピング統計情報とその説明を示します。

表 2-28 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	DHCP スヌーピングで処理されるパケットの合計数。転送パケットとドロップされたパケットを含みます。
Packets Dropped Because IDB not known	パケットの入力インターフェイスが不明なために発生したエラー数。
Queue full	パケット生成に使用する内部キューが満杯のために発生したエラー数。DHCP パケットが非常に高いレートで受信され、レートリミットが入力ポートでイネーブルになっていない場合に、このような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、そのパケットがあと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。
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、クライアントがスイッチ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。

表 2-28 DHCP スヌーピング統計情報 (続き)

DHCP スヌーピング統計情報	説明
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どちらかで、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。

関連コマンド	コマンド	説明
	clear ip dhcp snooping	DHCP スヌーピング バインディング データベース カウンタ、DHCP スヌーピング バインディング データベース エージェント統計情報カウンタ、DHCP スヌーピング統計情報カウンタをクリアします。

show ip igmp profile

すべての設定済インターネット グループ管理プロトコル (IGMP) プロファイルまたは指定した IGMP プロファイルを表示するには、**show ip igmp profile** 特権 EXEC コマンドを使用します。

show ip igmp profile [*profile number*] [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>profile number</i>	(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は、すべての IGMP プロファイルが表示されます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、プロファイル番号を指定した場合と指定しない場合の **show ip igmp profile** 特権 EXEC コマンドの出力を示します。プロファイル番号が入力されていない場合、表示にはスイッチ上で設定されたすべてのプロファイルが含まれます。

```
Switch# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255

Switch# 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
```

関連コマンド

コマンド	説明
ip igmp profile	特定の IGMP プロファイル番号を設定します。

show ip igmp snooping

スイッチまたは VLAN の IGMP スヌーピング設定を表示するには、**show ip igmp snooping** ユーザ EXEC コマンドを使用します。

```
show ip igmp snooping [groups | mrouter | querier] [vlan vlan-id] [ | {begin | exclude | include} expression]
```

シンタックスの説明

groups	(任意) show ip igmp snooping groups コマンドを参照してください。
mrouter	(任意) show ip igmp snooping mrouter コマンドを参照してください。
querier	(任意) show ip igmp snooping querier コマンドを参照してください。
vlan <i>vlan-id</i>	(任意) VLAN を指定します。範囲は 1 ~ 1001 および 1006 ~ 4094 です (特権 EXEC モードでのみ使用可能)。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定の VLAN の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。

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。

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

次の例では、**show ip igmp snooping vlan 1** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Switch# 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
Last member query interval   : 100

Vlan 1:
-----
IGMP snooping                :Enabled
```

show ip igmp snooping

```

Immediate leave                :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode     :IGMP_ONLY
Last member query interval    : 100

```

次の例では、**show ip igmp snooping** コマンドの出力を示します。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。

```

Switch> 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
Last member query interval    : 100

Vlan 1:
-----
IGMP snooping                :Enabled
Immediate leave              :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode     :IGMP_ONLY
Last member query interval    : 100

Vlan 2:
-----
IGMP snooping                :Enabled
Immediate leave              :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode     :IGMP_ONLY
Last member query interval    : 333

<output truncated>

```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping last-member-query-interval	IGMP スヌーピングの設定可能な Leave タイマーをイネーブルにします。
ip igmp snooping querier	レイヤ 2 ネットワークの IGMP クエリア機能をイネーブルにします。
ip igmp snooping report-suppression	IGMP レポート抑制をイネーブルにします。
ip igmp snooping tcn	IGMP トポロジ変更通知動作を設定します。
ip igmp snooping tcn flood	IGMP トポロジ変更通知動作としてマルチキャスト フラッディングを指定します。
ip igmp snooping vlan immediate-leave	VLAN の IGMP スヌーピング即時脱退処理をイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを追加、またはマルチキャストの学習方式を設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをマルチキャスト グループのメンバーとして静的に追加します。

コマンド	説明
<code>show ip igmp snooping groups</code>	スイッチの IGMP スヌーピング マルチキャスト テーブルを表示します。
<code>show ip igmp snooping mrouter</code>	スイッチまたは指定のマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。
<code>show ip igmp snooping querier</code>	スイッチ上に設定された IGMP クエリアの設定および動作情報を表示します。

show ip igmp snooping groups

スイッチの IGMP スヌーピング マルチキャスト テーブルを表示するか、またはマルチキャスト情報を表示するには、**show ip igmp snooping groups** 特権 EXEC コマンドを使用します。指定されたマルチキャスト VLAN のマルチキャスト テーブル、または特定のマルチキャスト情報を表示するには、**vlan** キーワードを使用します。

```
show ip igmp snooping groups [count | dynamic [count] | user [count]] [| {begin |
exclude | include} expression]
```

```
show ip igmp snooping groups vlan vlan-id [ip_address | count | dynamic [count] | user
[count]] [| {begin | exclude | include} expression]
```

シンタックスの説明

count	(任意) 実エントリの代わりに、指定のコマンド オプションのエントリ総数を表示します。
dynamic	(任意) IGMP スヌーピングにより学習したエントリを表示します。
user	(任意) ユーザ設定のマルチキャスト エントリのみ表示します。
ip_address	(任意) 指定グループ IP アドレスのマルチキャスト グループの特性を表示します。
vlan vlan-id	(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。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

マルチキャスト情報またはマルチキャスト テーブルを表示するには、このコマンドを使用します。

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。

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 次の例では、キーワードの指定をしない **show ip igmp snooping groups** コマンドの出力を示します。スイッチのマルチキャスト テーブルが表示されます。

```
Switch# show ip igmp snooping groups
Vlan      Group          Type          Version      Port List
-----
104       224.1.4.2      igmp          v2           Gi0/1, Gi0/2
104       224.1.4.3      igmp          v2           Gi0/1, Gi0/2
```

次の例では、**show ip igmp snooping groups count** コマンドの出力を示します。スイッチ上のマルチキャスト グループの総数が表示されます。

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

次の例では、**show ip igmp snooping groups dynamic** コマンドの出力を示します。IGMP スヌーピングにより学習したエントリのみを表示します。

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group          Type          Version      Port List
-----
104       224.1.4.2      igmp          v2           Gi0/1, Fa0/15
104       224.1.4.3      igmp          v2           Gi0/1, Fa0/15
```

次の例では、**show ip igmp snooping groups vlan vlan-id ip-address** コマンドの出力を示します。指定の IP アドレスのグループのエントリを表示します。

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group          Type          Version      Port List
-----
104       224.1.4.2      igmp          v2           Gi0/1, Fa0/15
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを設定します。
ip igmp snooping vlan static	レイヤ 2 ポートをマルチキャスト グループのメンバーとして静的に追加します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。
show ip igmp snooping mrouter	スイッチまたは指定のマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。

show ip igmp snooping mrouter

スイッチまたは指定されたマルチキャスト VLAN に対して動的に学習された IGMP スヌーピングと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、**show ip igmp snooping mrouter** 特権 EXEC コマンドを使用します。

```
show ip igmp snooping mrouter [vlan vlan-id] [| {begin | exclude | include} expression]
```

シンタックスの説明

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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定の VLAN 上のマルチキャスト ルータ ポートを表示するには、このコマンドを使用します。

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。

Multicast VLAN Registration (MVR; マルチキャスト VLAN レジストレーション) 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。

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

次の例では、**show ip igmp snooping mrouter** コマンドの出力を示します。スイッチ上でマルチキャスト ルータ ポートを表示します。

```
Switch# show ip igmp snooping mrouter
Vlan      ports
----      -
1         Gi0/1(dynamic)
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan mrouter	マルチキャスト ルータ ポートを追加します。
ip igmp snooping vlan static	レイヤ 2 ポートをマルチキャスト グループのメンバーとして静的に追加します。
show ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピング設定を表示します。
show ip igmp snooping groups	スイッチまたは指定のパラメータの IGMP スヌーピング マルチキャスト情報を表示します。

show ip igmp snooping querier

スイッチ上に設定された IGMP クエリアの設定と動作情報を表示するには、**show ip igmp snooping querier detail** ユーザ EXEC コマンドを使用します。

```
show ip igmp snooping querier [detail | vlan vlan-id [detail]] [ | {begin | exclude | include}
expression ]
```

シンタックスの説明

detail	(任意) IGMP クエリアの詳細情報を表示します。
vlan <i>vlan-id</i> [detail]	(任意) 指定された VLAN の IGMP クエリア情報を表示します。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。詳細を表示するには、 detail キーワードを使用します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

クエリアとも呼ばれ、IGMP クエリーメッセージを送信する検出装置の IGMP バージョンおよび 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 スイッチを指定できます。

show ip igmp snooping querier コマンド出力でも、検出されたクエリアの VLAN およびインターフェイスを表示します。クエリアがスイッチの場合は、コマンド出力の *Port* フィールドに *Router* と表示されます。クエリアがルータの場合は、出力の *Port* フィールドに、クエリアを学習したポートの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** コマンドに類似しています。ただし、**show ip igmp snooping querier** コマンドでは、スイッチクエリアにより直前に検出されたデバイス IP アドレスのみが表示されます。

show ip igmp snooping querier detail コマンドは、スイッチ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、次の追加情報を表示します。

- VLAN で選択されている IGMP クエリア
- VLAN で設定されたスイッチクエリア (ある場合) に関連する設定および動作情報

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

次の例では、**show ip igmp snooping querier** コマンドの出力を示します。

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11   v3                 Gi0/1
2         172.20.40.20   v2                 Router
```

次の例では、**show ip igmp snooping querier detail** コマンドの出力を示します。

```
Switch> show ip igmp snooping querier detail

Vlan      IP Address      IGMP Version      Port
-----
1         1.1.1.1         v2                 Fa0/1

Global IGMP switch 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 switch querier status
-----
elected querier is 1.1.1.1      on port Fa0/1
-----
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
```

関連コマンド

コマンド	説明
ip igmp snooping	スイッチまたは VLAN の IGMP スヌーピングをイネーブルにします。
ip igmp snooping querier	レイヤ 2 ネットワークの IGMP クエリア機能をイネーブルにします。
show ip igmp snooping	スイッチまたは指定のマルチキャスト VLAN の IGMP スヌーピング マルチキャスト ルータ ポートを表示します。

show ip source binding

スイッチ上の IP ソース バインディングを表示するには、**show ip source binding** ユーザ EXEC コマンドを使用します。

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *interface-id*] [**vlan** *vlan-id*] [| **{begin** | **exclude** | **include**} *expression*]

シンタックスの説明

<i>ip-address</i>	(任意) 特定の IP アドレスの IP ソース バインディングを表示します。
<i>mac-address</i>	(任意) 特定の MAC アドレスの IP ソース バインディングを表示します。
dhcp-snooping	(任意) DHCP スヌーピングで学習された IP ソース バインディングを表示します。
static	(任意) スタティック IP ソース バインディングを表示します。
interface <i>interface-id</i>	(任意) 特定のインターフェイス上の IP ソース バインディングを表示します。
vlan <i>vlan-id</i>	(任意) 特定の VLAN 上の IP ソース バインディングを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

show ip source binding コマンドの出力には、DHCP スヌーピング バインディング データベース内のダイナミックおよびスタティックに設定されたバインディングが表示されます。ダイナミックに設定されたバインディングだけを表示するには、**show ip dhcp snooping binding** 特権 EXEC コマンドを使用します。

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

次の例では、**show ip source binding** コマンドの出力を示します。

```
Switch> show ip source binding
MacAddress      IpAddress      Lease(sec)    Type           VLAN  Interface
-----
00:00:00:0A:00:0B  11.0.0.1      infinite      static         10    GigabitEthernet0/1
00:00:00:0A:00:0A  11.0.0.2      10000         dhcp-snooping  10    GigabitEthernet0/1
```

関連コマンド	コマンド	説明
	ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを設定します。
	ip source binding	スイッチ上のスタティック IP ソース バインディングを表示します。

show ip verify source

スイッチまたは特定のインターフェイス上の IP ソース ガード設定を表示するには、**show ip verify source** ユーザ EXEC コマンドを使用します。

```
show ip verify source [interface interface-id] [| {begin | exclude | include} expression]
```

シンタックスの説明

interface interface-id	(任意) 特定のインターフェイス上の IP ソース ガード設定を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show ip verify source** コマンドの出力を示します。

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----  -
gi0/1     ip           active       10.0.0.1        -----
gi0/1     ip           active       deny-all       11-20
gi0/2     ip           inactive-trust-port
gi0/3     ip           inactive-no-snooping-vlan
gi0/4     ip-mac      active       10.0.0.2        aaaa.bbbb.cccc  10
gi0/4     ip-mac      active       11.0.0.1        aaaa.bbbb.cccd  11
gi0/4     ip-mac      active       deny-all       deny-all        12-20
gi0/5     ip-mac      active       10.0.0.3        permit-all      10
gi0/5     ip-mac      active       deny-all       permit-all      11-20
```

上記の例にある IP ソース ガード設定は次のとおりです。

- ギガビットイーサネット 0/1 インターフェイス上で、VLAN 10 ~ 20 に対して DHCP スヌーピングがイネーブルになっています。VLAN 10 では、IP アドレス フィルタリングによる IP ソース ガードがインターフェイスに対して設定されており、バインディングがインターフェイス上に存在します。VLAN 11 ~ 20 では、2 番目のエントリに、デフォルト ポートが IP ソース ガードが設定されていない VLAN のインターフェイスに適用されていることが示されています。
- ギガビットイーサネット 0/2 インターフェイスは、DHCP スヌーピングを実行するための信頼できるインターフェイスとして設定されています。

- ギガビット イーサネット 0/3 インターフェイス上で、インターフェイスが属している VLAN に対して DHCP スヌーピングがイネーブルになっていません。
- ギガビット イーサネット 0/4 インターフェイス上で、送信元 IP アドレス フィルタリングと送信元 MAC アドレス フィルタリングによる IP ソース ガードがイネーブルになっており、VLAN 10 と VLAN 11 に対してスタティック IP ソース バインディングが設定されています。VLAN 12 ~ 20 では、IP ソース ガードが設定されていない VLAN のインターフェイスにデフォルト ポート ACL が適用されています。
- ギガビット イーサネット 0/5 インターフェイス上で、送信元 IP アドレス フィルタリングと送信元 MAC アドレス フィルタリングによる IP ソース ガードがイネーブルになっており、スタティック IP バインディングが設定されていますが、ポート セキュリティがディセーブルになっています。スイッチは送信元 MAC アドレスのフィルタリングを実行できません。

次の例では、IP ソース ガードがディセーブルになっているインターフェイスに対する出力を示します。

```
Switch> show ip verify source gigabitethernet0/6
IP source guard is not configured on the interface gi0/6.
```

関連コマンド

コマンド	説明
ip verify source	インターフェイス上で IP ソース ガードをイネーブルにします。

show ipv6 mld snooping

スイッチまたは VLAN の IP Version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピング設定を表示するには、**show ipv6 mld snooping** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping [*vlan vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

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 {default}** 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。

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

次の例では、**show ipv6 mld snooping vlan** コマンドの出力を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Switch> 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

```

次の例では、**show ipv6 mld snooping** コマンドの出力を示します。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。

```

Switch> 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

<テキスト出力は省略>

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

```

関連コマンド

コマンド	説明
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に SDM テンプレートを設定します。

show ipv6 mld snooping address

Multicast Listener Discovery (MLD) スヌーピングで保持されるすべての IP Version 6 (IPv6) マルチキャストアドレス情報または指定の IPv6 マルチキャストアドレス情報を表示するには、**show ipv6 mld snooping address** ユーザ EXEC コマンドを使用します。

```
show ipv6 mld snooping address [[vlan vlan-id] [ipv6 address]] [vlan vlan-id] [count |
dynamic | user] [| {begin | exclude | include} expression]
```



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

vlan vlan-id	(任意) MLD スヌーピング マルチキャストアドレス情報を表示する VLAN を指定します。指定できる VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。
ipv6-multicast-address	(任意) 指定された IPv6 マルチキャストアドレスに関する情報を表示します。このキーワードは、VLAN ID を指定した場合にのみ使用できます。
count	(任意) スイッチ上または指定の VLAN のマルチキャストグループ数を表示します。
dynamic	(任意) MLD スヌーピング学習グループ情報を表示します。
user	(任意) MLD スヌーピング ユーザ設定グループ情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

IPv6 マルチキャストアドレス情報を表示するのに、このコマンドを使用します。

VLAN ID を入力したあとでのみ、IPv6 マルチキャストアドレスを入力できます。

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。

学習されたグループに関する情報のみを表示するには、**dynamic** キーワードを使用します。設定されたグループに関する情報のみを表示するには、**user** キーワードを使用します。

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 {default 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。

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

次の例では、**show snooping address** ユーザ EXEC コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address
Vlan Group   Type Version Port List
-----
2    FF12::3 user           Fa0/2, Gi0/2, Gi0/1,Gi0/3
EX
```

次の例では、**show snooping address count** ユーザ EXEC コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address count
Total number of multicast groups: 2
```

次の例では、**show snooping address user** ユーザ EXEC コマンドの出力を示します。

```
Switch> show ipv6 mld snooping address user
Vlan Group   Type Version Port List
-----
2    FF12::3 user   v2    Fa0/2, Gi0/2, Gi0/1,Gi0/3
```

関連コマンド

コマンド	説明
ipv6 mld snooping vlan	VLAN で IPv6 MLD スヌーピングを設定します。
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 snooping mrouter

スイッチまたは VLAN に対して動的に学習され、手動で設定された IP Version 6 (IPv6) Multicast Listener Discovery (MLD) ルータ ポートを表示するには、**show ipv6 mld snooping mrouter** ユーザ EXEC コマンドを使用します。

show ipv6 mld snooping mrouter [*vlan vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

スイッチまたは特定の VLAN の MLD スヌーピング ルータ ポートを表示するには、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 default** 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。

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

次の例では、**show ipv6 mld snooping mrouter** コマンドの出力を示します。ここでは、スイッチ上で MLD スヌーピングに参加しているすべての VLAN のスヌーピング特性が表示されます。

```
Switch> show ipv6 mld snooping mrouter
Vlan      ports
-----
2         Gi0/11 (dynamic)
72        Gi0/11 (dynamic)
200       Gi0/11 (dynamic)
```

次の例では、**show ipv6 mld snooping mrouter vlan** コマンドの出力を示します。ここでは、特定の VLAN のマルチキャスト ルータ ポートが表示されます。

```
Switch> show ipv6 mld snooping mrouter vlan 100
Vlan      ports
-----
 2        Gi0/11 (dynamic)
```

関連コマンド

コマンド	説明
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。
ipv6 mld snooping vlan mrouter interface interface-id static ipv6-multicast-address interface interface-id]	VLAN のマルチキャスト ルータ ポートを設定します。
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に SDM テンプレートを設定します。

show ipv6 mld snooping querier

スイッチまたは VLAN が受信した最新の IP Version 6 (IPv6) Multicast Listener Discovery (MLD) スヌーピング クエリア関連情報を表示するには、**show ipv6 mld snooping querier** ユーザ EXEC コマンドを使用します。

```
show ipv6 mld snooping querier [vlan vlan-id] [detail] [ | {begin | exclude | include}
expression]
```



(注)

このコマンドを使用するには、スイッチで LAN Base イメージが動作していて、デュアル IPv4 および IPv6 Switch Database Management (SDM) テンプレートが設定されている必要があります。

シンタックスの説明

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。
detail	(任意) スイッチまたは VLAN の MLD スヌーピングの詳細なクエリア情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

MLD クエリー メッセージを送信する検出された装置 (クエリアとも呼ばれる) の MLD バージョンおよび IPv6 アドレスを表示するには、**show ipv6 mld 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 ルータを持つことができますが、MLD クエリアは 1 つだけです。クエリアには、レイヤ 3 スイッチを指定できます。

show ipv6 mld snooping querier コマンド出力は、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します。クエリアがスイッチの場合は、コマンド出力の **Port** フィールドに **Router** と表示されます。クエリアがルータの場合は、出力の **Port** フィールドに、クエリアを学習したポートの番号が表示されます。

show ipv6 mld snoop querier vlan コマンドの出力では、外部または内部クエリアからのクエリー メッセージにตอบสนองして受信された情報を表示します。特定の VLAN 上のスヌーピング ロバストネス変数などのユーザ設定の VLAN 値は表示されません。このクエリア情報は、スイッチが送信する MASQ メッセージ上でのみ使用します。クエリー メッセージにตอบสนองしないメンバーを期限切れにするのに使用するユーザ設定のロバストネス変数は無効にはなりません。

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 {default}** 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。

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

次の例では、**show ipv6 mld snooping querier** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address          MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi0/1
```

次の例では、**show ipv6 mld snooping querier detail** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier detail
Vlan      IP Address          MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi0/1
```

次の例では、**show ipv6 mld snooping querier vlan** コマンドの出力を示します。

```
Switch> show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Port : Gi0/1
Max response time : 1000s
```

関連コマンド

コマンド	説明
ipv6 mld snooping	スイッチ上または VLAN 上の IPv6 MLD スヌーピングをイネーブルにし、設定を行います。
ipv6 mld snooping last-listener-query-count	MLD クライアントが期限切れになる前にスイッチが送信するクエリアの最大数を設定します。
ipv6 mld snooping last-listener-query-interval	スイッチがクエリーを送信してから、マルチキャスト グループからポートを削除する前に待機する最大応答時間を設定します。
ipv6 mld snooping robustness-variable	応答がない場合、マルチキャスト アドレスが期限切れになる前にスイッチが送信するクエリーの最大数を設定します。
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に SDM テンプレートを設定します。
ipv6 mld snooping	スイッチ上または VLAN 上の IPv6 MLD スヌーピングをイネーブルにし、設定を行います。

show ipv6 route updated

IPv6 ルーティング テーブルの現在の内容を表示するには、**show ipv6 route updated** ユーザ EXEC コマンドを使用します。

```
show ipv6 route [protocol] updated [boot-up] {hh:mm | day{month [hh:mm]} [ {hh:mm | day{month [hh:mm]} ] [ {begin | exclude | include} expression]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>protocol</i>	(任意) 次のいずれかのキーワードを使用して指定したルーティングプロトコルのルートを表示します。 <ul style="list-style-type: none"> • bgp • isis • ospf • rip または、次のいずれかのキーワードを使用して指定したルートタイプのルートを表示します。 <ul style="list-style-type: none"> • connected • local • static • interface <i>interface id</i>
boot-up	IPv6 ルーティング テーブルの現在の内容を表示します。
<i>hh:mm</i>	24 時間表記の 2 桁の数値で時刻を入力します。必ずコロン (:) を使用してください。たとえば、 13:32 のように入力します。
<i>day</i>	日にちを入力します。指定できる範囲は 1 ~ 31 です。
<i>month</i>	月を大文字または小文字で入力します。 January または august など、月の名前をすべて入力することも、 jan または Aug のように月の名前の最初の 3 文字を入力することもできます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

IPv6 ルーティング テーブルの現在の内容を表示するには、**show ipv6 route** 特権 EXEC コマンドを使用します。

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

次の例では、**show ipv6 route updated rip** コマンドの出力を示します。

```
Switch> show ipv6 route rip updated
IPv6 Routing Table - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
IA - ISIS interarea, IS - ISIS summary
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:8D01, GigabitEthernet0/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/4
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/5
Last updated 17:23:05 22 February 2007
```

関連コマンド

コマンド	説明
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。構文情報については、「Cisco IOS Software」>「Command References for the Cisco IOS Software Releases 12.3 Mainline」>「Cisco IOS IPv6 Command Reference」>「IPv6 Commands: show ipv6 nat translations through show ipv6 protocols」を選択してください。

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、**show lacp** ユーザ EXEC コマンドを使用します。

```
show lacp [channel-group-number] {counters | internal | neighbor | sys-id} [| {begin |
exclude | include} expression]
```

シンタックスの説明

<i>channel-group-number</i>	(任意) チャンネル グループの番号です。指定できる範囲は 1 ~ 6 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	ネイバー情報を表示します。
sys-id	LACP で使用されるシステム ID を表示します。システム ID は、LACP システム プライオリティおよびスイッチ MAC (メディア アクセス制御) アドレスで構成されています。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。指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 オプションを入力することで、**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。

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

次の例では、**show lacp counters** ユーザ EXEC コマンドの出力を示します。表 2-29 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show lacp counters
          LACPDUs      Marker      Marker Response      LACPDUs
Port      Sent  Recv      Sent  Recv      Sent  Recv      Pkts Err
-----
Channel group:1
Gi0/1      19    10         0     0         0     0         0
Gi0/2      14     6         0     0         0     0         0
```

表 2-29 show lacp counters のフィールドの説明

フィールド	説明
LACPDUs 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
LACPDUs 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

次の例では、**show lacp internal** コマンドの出力を示します。

```
Switch> 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
Port      Flags   State   Priority    Key     Key   Number State
Gi0/1     SA      bndl    32768       0x3     0x3   0x4    0x3D
Gi0/2     SA      bndl    32768       0x3     0x3   0x5    0x3D
```

表 2-30 に、この出力で表示される各フィールドの説明を示します。

表 2-30 show lacp internal のフィールドの説明

フィールド	説明
State	指定のポートの状態。次に使用可能な値を示します。 <ul style="list-style-type: none"> – : ポートが unknown ステートです。 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 : ポートをその他ポートとともにバンドルできません。 indep : ポートは independent ステートです。バンドルされませんがデータトラフィックを切り替えます。この場合、LACP は相手側ポートで稼動していません。 down : ポートがダウンしています。
LACP Port Priority	ポートのプライオリティ設定。互換性のあるすべてのポートが集約することを回避するため、ハードウェアの制限がある場合、LACP はポートプライオリティによりポートをスタンバイモードにします。
Admin Key	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)。管理用のキーは、ポートが他のポートと集約できる能力を定義します。他のポートと集約できるポートの能力は、ポートの物理特性 (データ転送速度やデュプレックス機能など) と設定した制限によって決まります。

表 2-30 show lacp internal のフィールドの説明 (続き)

フィールド	説明
Oper Key	ポートで使用されるランタイムの操作キー。LACP は自動的に値を生成します (16 進数)。
Port Number	ポート番号。
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、メッセージは次のようになります。</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>(注) 上のリストでは、bit7 が MSB で bit0 は LSB です。</p>

次の例では、**show lacp neighbor** コマンドの出力を示します。

```
Switch> 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:
```

```

Partner          Partner          Partner          Partner
Port             System ID       Port Number      Age             Flags
Gi0/1           32768,0007.eb49.5e80 0xC              19s            SP

LACP Partner    Partner          Partner
Port Priority    Oper Key         Port State
32768           0x3             0x3C
```

```
Partner's information:
```

```

Partner          Partner          Partner          Partner
Port             System ID       Port Number      Age             Flags
Gi0/2           32768,0007.eb49.5e80 0xD              15s            SP

LACP Partner    Partner          Partner
Port Priority    Oper Key         Port State
32768           0x3             0x3C
```

次の例では、**show lacp sys-id** コマンドの出力を示します。

```
Switch> 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。

関連コマンド

コマンド	説明
clear lacp	LACP チャンネル グループ情報を消去します。
lacp port-priority	LACP ポート プライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。

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、**show location** ユーザ EXEC コマンドを使用します。

```
show location admin-tag [ [ { begin | exclude | include } expression ]
```

```
show location civic-location { identifier id number | interface interface-id | static } | { begin | exclude | include } expression]
```

```
show location elin-location { identifier id number | interface interface-id | static } | { begin | exclude | include } expression]
```

シンタックスの説明

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表示します。
elin-location	緊急ロケーション情報 (ELIN) を表示します。
identifier <i>id</i>	都市ロケーションまたは elin ロケーションの ID を指定します。指定できる ID 範囲は 1 ~ 4095 です。
interface <i>interface-id</i>	(任意) 指定されたインターフェイスまたはすべてのインターフェイスに対するロケーション情報を表示します。指定できるインターフェイスとして、物理ポートも含まれます。
static	スタティック コンフィギュレーション情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

エンドポイントのロケーション情報を表示するには、**show location** コマンドを使用します。

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

次の例では、インターフェイスのロケーション情報を表示する **show location civic-location** コマンドの出力を示します。

```
Switch> show location civic interface gigibitethernet0/1
Civic location information
-----
Identifier           : 1
County              : Santa Clara
```



```
Street number      : 3550
Building           : 19
Room               : C6
Primary road name  : Cisco Way
City               : San Jose
State              : CA
Country            : US
```

次の例では、すべての都市ロケーション情報を表示する **show location civic-location** コマンドの出力を示します。

```
Switch> show location civic-location static
Civic location information
-----
Identifier         : 1
County             : Santa Clara
Street number      : 3550
Building           : 19
Room               : C6
Primary road name  : Cisco Way
City               : San Jose
State              : CA
Country            : US
Ports              : Gi0/1
-----
Identifier         : 2
Street number      : 24568
Street number suffix : West
Landmark           : Golden Gate Bridge
Primary road name  : 19th Ave
City               : San Francisco
Country            : US
-----
```

次の例では、緊急ロケーション情報を表示する **show location elin-location** コマンドの出力を示します。

```
Switch> show location elin-location identifier 1
Elin location information
-----
Identifier : 1
Elin       : 14085553881
Ports      : Gi0/2
```

次の例では、すべての緊急ロケーション情報を表示する **show location elin static** コマンドの出力を示します。

```
Switch> show location elin static
Elin location information
-----
Identifier : 1
Elin       : 14085553881
Ports      : Gi0/2
-----
Identifier : 2
Elin       : 18002228999
-----
```

■ show location

関連コマンド

コマンド	説明
location (グローバル コンフィギュレーション)	エンドポイントにグローバル ロケーション情報を設定します。
location (インターフェイス コンフィギュレーション)	インターフェイスにロケーション情報を設定します。

show link state group

リンクステート グループ情報を表示するには、**show link state group** 特権 EXEC コマンドを使用します。

```
show link state group [number] [detail] [| {begin | exclude | include} expression]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>number</i>	(任意) リンクステート グループの番号です。
detail	(任意) 詳細情報を表示するよう指定します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

デフォルト

デフォルトはありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

リンクステート グループ情報を表示するには、**show link state group** コマンドを使用します。キーワードを指定しないでこのコマンドを使用すると、すべてのリンクステート グループの情報が表示されます。特定のグループの情報を表示するには、グループ番号を入力します。

グループの詳細情報を表示するには、**detail** キーワードを使用します。**show link state group detail** コマンドの出力では、リンクステート トラッキングがイネーブルになっているか、またはアップストリームまたはダウンストリーム (あるいはその両方) インターフェイスが設定されたリンクステートグループだけが表示されます。グループにリンクステート グループ設定がない場合、イネーブルまたはディセーブルとして表示されません。

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

次の例では、**show link state group 1** コマンドの出力を示します。

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

■ show link state group

次の例では、**show link state group detail** コマンドの出力を示します。

```
Switch> show link state group detail
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn) Gi0/17(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

関連コマンド

コマンド	説明
link state group	リンクステート グループのメンバーとしてインターフェイスを設定します。
link state track	リンクステート グループをイネーブルにします。
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference for Release 12.2」 > 「Cisco IOS File Management Commands」 > 「Configuration File Commands」 を選択してください。

show mac access-group

特定のインターフェイスまたはスイッチに設定されている MAC アクセス コントロール リスト (ACL) を表示するには、**show mac access-group** ユーザ EXEC コマンドを使用します。

show mac access-group [*interface interface-id*] [| {**begin** | **exclude** | **include**} *expression*]



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

interface <i>interface-id</i>	(任意) 特定のインターフェイスで設定された MAC ACL を表示します。有効なインターフェイスは物理ポートとポート チャネルです。ポート チャネル範囲は 1 ~ 6 です (特権 EXEC モードでのみ使用可能)。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac-access group** ユーザ EXEC コマンドの出力を示します。ポート 2 には、適用される MAC アクセス リスト *macl_e1* があります。MAC ACL は他のインターフェイスに適用されません。

```
Switch> show mac access-group
Interface GigabitEthernet0/1:
  Inbound access-list is not set
Interface GigabitEthernet0/2:
  Inbound access-list is macl_e1
Interface GigabitEthernet0/3:
  Inbound access-list is not set
Interface GigabitEthernet0/4:
  Inbound access-list is not set
```

<output truncated>

次の例では、**show mac access-group interface** コマンドの出力を示します。

```
Switch# show mac access-group interface gigabitethernet0/1
Interface GigabitEthernet0/1:
  Inbound access-list is macl_e1
```

■ show mac access-group

関連コマンド	コマンド	説明
	mac access-group	インターフェイスに MAC アクセス グループを適用します。

show mac address-table

指定の MAC（メディア アクセス制御）アドレス テーブルのダイナミック/スタティック エントリ、または指定のインターフェイスや VLAN 上の MAC アドレス テーブルのダイナミック/スタティック エントリを表示するには、**show mac address-table** ユーザ EXEC コマンドを使用します。

show mac address-table [| {begin | exclude | include} expression]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac address-table** コマンドの出力を示します。

```
Switch> show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0000.0000.0001   STATIC  CPU
All     0000.0000.0002   STATIC  CPU
All     0000.0000.0003   STATIC  CPU
All     0000.0000.0009   STATIC  CPU
All     0000.0000.0012   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
1       0030.9441.6327   DYNAMIC Gi0/4
Total Mac Addresses for this criterion: 12
```

関連コマンド

コマンド	説明
clear mac address-table dynamic	MAC アドレス テーブルから、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、または特定の VLAN 上のすべてのダイナミック アドレスを削除します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	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。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table address

指定した MAC アドレスの MAC アドレス テーブル情報を表示するには、**show mac address-table address** ユーザ EXEC コマンドを使用します。

```
show mac address-table address mac-address [interface interface-id] [vlan vlan-id] [ |
  {begin | exclude | include} expression]
```

シンタックスの説明

<i>mac-address</i>	48 ビットの MAC アドレスを指定します。有効な形式は H.H.H です。
interface <i>interface-id</i>	(任意) 特定のインターフェイスの情報を表示します。有効なインターフェイスは、物理ポートおよびポート チャネルです。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のみ、エントリを表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac address-table address** コマンドの出力を示します。

```
Switch# show mac address-table address 0002.4b28.c482
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0002.4b28.c482  STATIC CPU
Total Mac Addresses for this criterion: 1
```

関連コマンド

コマンド	説明
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	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。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table aging-time

特定のアドレス テーブル インスタンスのエージング タイム、特定の VLAN 上または指定がない場合はすべての VLAN 上のすべてのアドレス テーブル インスタンスのエージング タイムを表示するには、**show mac address-table aging-time** ユーザ EXEC コマンドを使用します。

```
show mac address-table aging-time [vlan vlan-id] [| {begin | exclude | include} expression]
```

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 特定の VLAN のエージング タイム情報を表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VLAN 番号が指定されない場合、すべての VLAN に対するエージング タイムが表示されます。

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

次の例では、**show mac address-table aging-time** コマンドの出力を示します。

```
Switch> show mac address-table aging-time
Vlan      Aging Time
-----
1         300
```

次の例では、**show mac address-table aging-time vlan 10** コマンドの出力を示します。

```
Switch> show mac address-table aging-time vlan 10
Vlan      Aging Time
-----
10        300
```

関連コマンド

コマンド	説明
mac address-table aging-time	ダイナミック エントリが使用または更新された後、MAC（メディア アクセス制御）アドレス テーブル内に保持される時間を設定します。
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	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。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table count

すべての VLAN または指定の VLAN に存在するアドレス数を表示するには、**show mac address-table count** ユーザ EXEC コマンドを使用します。

```
show mac address-table count [vlan vlan-id] [| {begin | exclude | include} expression]
```

シンタックスの説明	
vlan <i>vlan-id</i>	(任意) 特定の VLAN のアドレス数を表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード ユーザ EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン VLAN 番号が指定されない場合、すべての VLAN に対するアドレス カウントが表示されます。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 次の例では、**show mac address-table count** コマンドの出力を示します。

```
Switch# show mac address-table count
Mac Entries for Vlan : 1
-----
Dynamic Address Count : 2
Static Address Count : 0
Total Mac Addresses : 2
```

関連コマンド

コマンド	説明
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	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。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table dynamic

ダイナミックな MAC（メディア アクセス制御）アドレス テーブル エントリのみを表示するには、**show mac address-table dynamic** ユーザ EXEC コマンドを使用します。

```
show mac address-table dynamic [address mac-address] [interface interface-id] [vlan
vlan-id]
[ | {begin | exclude | include} expression]
```

シンタックスの説明

address <i>mac-address</i>	(任意) 48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です (特権 EXEC モードでのみ利用可能)。
interface <i>interface-id</i>	(任意) マッチングを行う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としては、物理ポートおよびポート チャネルがあります。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のエントリを表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac address-table dynamic** コマンドの出力を示します。

```
Switch> show mac address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Gi0/2
1       00b0.6496.2741   DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

関連コマンド

コマンド	説明
clear mac address-table dynamic	MAC アドレス テーブルから、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、または特定の VLAN 上のすべてのダイナミック アドレスを削除します。
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table interface

指定の VLAN の指定のインターフェイスの MAC（メディア アクセス制御）アドレス テーブル情報を表示するには、**show mac address-table interface** ユーザ コマンドを使用します。

```
show mac address-table interface interface-id [vlan vlan-id] [| {begin | exclude | include}
expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) インターフェイス タイプを指定します。有効なインターフェイスとしては、物理ポートおよびポート チャネルがあります。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のエントリを表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac address-table interface** コマンドの出力を示します。

```
Switch> show mac address-table interface gigabitethernet0/2
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Gi0/2
1       00b0.6496.2741   DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

関連コマンド

コマンド	説明
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table notification	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。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table learning

すべての VLAN または指定した VLAN の MAC アドレス学習のステータスを表示するには、**show mac address-table learning** ユーザ EXEC コマンドを使用します。

show mac address-table learning [vlan *vlan-id*] [| {begin** | **exclude** | **include**} *expression*]**



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

vlan <i>vlan-id</i>	(任意) 特定の VLAN の情報を表示します。指定できる範囲は 1 ~ 4094 です。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(46)SE1	このコマンドが追加されました。

使用上のガイドライン

設定された VLAN と、その VLAN で MAC アドレス学習がイネーブルかディセーブルかを表示するには、キーワードを指定しないで **show mac address-table learning** コマンドを使用します。デフォルトは、すべての VLAN で MAC アドレス学習がイネーブルです。個々の VLAN の学習ステータスを表示するには、特定の VLAN ID を指定してこのコマンドを使用します。

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

次の例では、MAC アドレス学習が VLAN 200 でディセーブルになっていることを示す **show mac address-table learning** ユーザ EXEC コマンドの出力を示します。

```
Switch> show mac address-table learning
VLAN      Learning Status
----      -
1          yes
100       yes
200       no
```

関連コマンド

コマンド	説明
mac address-table learning vlan	VLAN の MAC アドレス学習をイネーブルまたはディセーブルにします。

show mac address-table move update

スイッチの MAC（メディア アクセス制御）アドレス テーブル移行更新の情報を表示するには、**show mac address-table move update** ユーザ EXEC コマンドを使用します。

show mac address-table move update [| {begin | exclude | include} expression]



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

begin	(任意) expression と一致する行から表示を開始します。
exclude	(任意) expression と一致する行を表示から除外します。
include	(任意) 指定された expression と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac address-table move update** コマンドの出力を示します。

```
Switch> 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
switch#
```

関連コマンド

コマンド	説明
<code>clear mac address-table move update</code>	MAC アドレス テーブル移行更新カウンタをクリアします。
<code>mac address-table move update {receive transmit}</code>	スイッチ上の MAC アドレス テーブル移行更新を設定します。

show mac address-table notification

すべてのインターフェイスまたは指定のインターフェイスの MAC（メディア アクセス制御）アドレス通知設定を表示するには、**show mac address-table notification** ユーザ EXEC コマンドを使用します。

```
show mac address-table notification [interface [interface-id]] [| {begin | exclude | include}
expression]
```

シンタックスの説明

interface	(任意) すべてのインターフェイスの情報を表示します。有効なインターフェイスは、物理ポートおよびポート チャネルです。
<i>interface-id</i>	(任意) 指定されたインターフェイスの情報を表示します。有効なインターフェイスは、物理ポートおよびポート チャネルです。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

キーワードを指定しないで **show mac address-table notification** コマンドを使用すると、機能がイネーブルかディセーブルか、MAC 通知間隔、履歴テーブルの最大許容エントリ数、および履歴テーブルの内容を表示します。

すべてのインターフェイスのフラグを表示するには、**interface** キーワードを使用します。*interface-id* が含まれる場合、指定したインターフェイスのフラグのみが表示されます。

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

次の例では、**show mac address-table notification** コマンドの出力を示します。

```
Switch> show mac address-table notification
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
-----
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0001 Module: 0   Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Added   Vlan: 2       MAC Addr: 0000.0000.0003 Module: 0   Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0001 Module: 0   Port: 1
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Deleted Vlan: 2       MAC Addr: 0000.0000.0003 Module: 0   Port: 1
```

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバルカウンタをクリアします。
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table static

スタティック MAC（メディア アクセス制御）アドレス テーブル エントリのみを表示するには、**show mac address-table static** ユーザ EXEC コマンドを使用します。

```
show mac address-table static [address mac-address] [interface interface-id] [vlan vlan-id]
[ | {begin | exclude | include} expression]
```

シンタックスの説明

address <i>mac-address</i>	(任意) 48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です (特権 EXEC モードでのみ利用可能)。
interface <i>interface-id</i>	(任意) マッチングを行う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としては、物理ポートおよびポート チャネルがあります。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のアドレスを表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac address-table static** コマンドの出力を示します。

```
Switch> show mac address-table static
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0100.0ccc.cccc   STATIC  CPU
All     0180.c200.0000   STATIC  CPU
All     0100.0ccc.cccd   STATIC  CPU
All     0180.c200.0001   STATIC  CPU
All     0180.c200.0004   STATIC  CPU
All     0180.c200.0005   STATIC  CPU
  4     0001.0002.0004   STATIC  Drop
  6     0001.0002.0007   STATIC  Drop
Total Mac Addresses for this criterion: 8
```

関連コマンド

コマンド	説明
mac address-table static	MAC アドレス テーブルにスタティック アドレスを追加します。
mac address-table static drop	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、特定の送信元または宛先 MAC アドレスを持つトラフィックをドロップするようにスイッチを設定します。
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	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。
show mac address-table vlan	特定の VLAN の MAC アドレス テーブル情報を表示します。

show mac address-table vlan

指定の VLAN の MAC (メディア アクセス制御) アドレス テーブル情報を表示するには、**show mac address-table vlan** ユーザ EXEC コマンドを使用します。

```
show mac address-table vlan vlan-id [ | {begin | exclude | include} expression]
```

シンタックスの説明

<i>vlan-id</i>	(任意) 特定の VLAN のアドレスを表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mac address-table vlan 1** コマンドの出力を示します。

```
Switch> show mac address-table vlan 1
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0100.0ccc.cccc  STATIC  CPU
1       0180.c200.0000  STATIC  CPU
1       0100.0ccc.cccd  STATIC  CPU
1       0180.c200.0001  STATIC  CPU
1       0180.c200.0002  STATIC  CPU
1       0180.c200.0003  STATIC  CPU
1       0180.c200.0005  STATIC  CPU
1       0180.c200.0006  STATIC  CPU
1       0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

関連コマンド

コマンド	説明
show mac address-table address	指定の MAC アドレスの MAC アドレス テーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface	特定のインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table notification	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。
show mac address-table static	スタティック MAC アドレス テーブル エントリのみを表示します。

show mls qos

グローバルな QoS (Quality of Service) 設定情報を表示するには、**show mls qos** ユーザ EXEC コマンドを使用します。

```
show mls qos [ | {begin | exclude | include} expression]
```

シンタックスの説明	
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード ユーザ EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン 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 次の例では、QoS がイネーブルで DSCP 透過もイネーブルの場合の **show mls qos** コマンドの出力を示します。

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

関連コマンド	コマンド	説明
	mls qos	スイッチ全体に対して QoS をイネーブルにします。

show mls qos aggregate-policer

QoS (Quality of Service) アグリゲート ポリサー設定を表示するには、**show mls qos aggregate-policer** ユーザ EXEC コマンドを使用します。ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。

```
show mls qos aggregate-policer [aggregate-policer-name] [| {begin | exclude | include}
expression]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>aggregate-policer-name</i>	(任意) 指定された名前のポリシー設定を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mls qos aggregate-policer** コマンドの出力を示します。

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

関連コマンド

コマンド	説明
mls qos aggregate-policer	ポリシー マップ内で複数のクラスが共有するポリサー パラメータを定義します。

show mls qos input-queue

入力キューの QoS (Quality of Service) を表示するには、**show mls qos input-queue** ユーザ EXEC コマンドを使用します。

```
show mls qos input-queue [ | {begin | exclude | include} expression]
```

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mls qos input-queue** コマンドの出力を示します。

```
Switch> show mls qos input-queue
Queue      :      1      2
-----
buffers    :      90     10
bandwidth  :       4      4
priority   :       0     10
threshold1:     100    100
threshold2:     100    100
```

関連コマンド

コマンド	説明
mls qos srr-queue input bandwidth	入力キューに対し Shaped Round Robin (SRR) ウェイトを割り当てます。
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input cos-map	割り当てられたサービス クラス (CoS) 値を入力キューにマッピングし、CoS 値をキューとしきい値 ID に割り当てます。
mls qos srr-queue input dscp-map	割り当てられた Differentiated Service Code Point (DSCP) 値を入力キューにマッピングし、DSCP 値をキューとしきい値 ID に割り当てます。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を保証します。
mls qos srr-queue input threshold	Weighted Tail-Drop (WTD) しきい値のパーセントを入力キューに割り当てます。

show mls qos interface

QoS (Quality of Service) 情報をポート レベルで表示するには、**show mls qos interface** ユーザ EXEC コマンドを使用します。

```
show mls qos interface [interface-id] [buffers | queueing | statistics]
[ | {begin | exclude | include} expression]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>interface-id</i>	(任意) 指定されたポートの QoS 情報を表示します。指定できるインターフェイスとして、物理ポートも含まれます。
buffers	(任意) キュー間のバッファ割り当てを表示します。
queueing	(任意) キューイングの指針 (共有またはシェーピング) およびキューに対応したウェイトを表示します。
statistics	(任意) 送受信された Differentiated Service Code Point (DSCP) 値とサービスクラス (CoS) 値、出力キュー単位でキューに入れられたパケット数または削除されたパケット数、およびポリサーごとのプロファイル内のパケット数とプロファイル外のパケット数の統計情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注)

policer 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。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、VLAN ベース QoS がイネーブルの場合の **show mls qos interface interface-id** コマンドの出力を示します。

```
Switch> show mls qos interface gigabitethernet0/1
GigabitEthernet0/1
```



```

trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:vlan-based

```

次の例では、VLAN ベース QoS がディセーブルの場合の **show mls qos interface interface-id** コマンドの出力を示します。

```

Switch> show mls qos interface gigabitethernet0/2
GigabitEthernet0/2
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:port-based

```

次の例では、**show mls qos interface interface-id buffers** コマンドの出力を示します。

```

Switch> show mls qos interface gigabitethernet0/2 buffers
GigabitEthernet0/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25

```

次の例では、**show mls qos interface interface-id queueing** コマンドの出力を示します。出力緊急キューは、設定された Shaped Round Robin (SRR) の重みを無効にします。

```

Switch> show mls qos interface gigabitethernet0/2 queueing
GigabitEthernet0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational Bandwidth:100.0)
The port is mapped to qset : 1

```

次の例では、**show mls qos interface interface-id statistics** コマンドの出力を示します。表 2-31 に、この出力で表示される各フィールドの説明を示します。

```

Switch> show mls qos interface gigabitethernet0/2 statistics
GigabitEthernet0/2

dscp: incoming
-----
 0 - 4 :      4213      0      0      0      0
 5 - 9 :         0      0      0      0      0
10 - 14 :         0      0      0      0      0
15 - 19 :         0      0      0      0      0
20 - 24 :         0      0      0      0      0
25 - 29 :         0      0      0      0      0
30 - 34 :         0      0      0      0      0
35 - 39 :         0      0      0      0      0
40 - 44 :         0      0      0      0      0
45 - 49 :         0      0      0      6      0
50 - 54 :         0      0      0      0      0
55 - 59 :         0      0      0      0      0
60 - 64 :         0      0      0      0      0
dscp: outgoing

```

show mls qos interface

```

-----
 0 - 4 :    363949      0      0      0      0
 5 - 9 :         0      0      0      0      0
10 - 14 :         0      0      0      0      0
15 - 19 :         0      0      0      0      0
20 - 24 :         0      0      0      0      0
25 - 29 :         0      0      0      0      0
30 - 34 :         0      0      0      0      0
35 - 39 :         0      0      0      0      0
40 - 44 :         0      0      0      0      0
45 - 49 :         0      0      0      0      0
50 - 54 :         0      0      0      0      0
55 - 59 :         0      0      0      0      0
60 - 64 :         0      0      0      0      0
  cos: incoming
-----
 0 - 4 :    132067      0      0      0      0
 5 - 9 :         0      0      0      0      0
  cos: outgoing
-----
 0 - 4 :    739155      0      0      0      0
 5 - 9 :         90      0      0      0      0

Policer: Inprofile:      0 OutofProfile:      0

```

表 2-31 show mls qos interface statistics のフィールドの説明

フィールド		説明
DSCP	incoming	DSCP 値ごとに受信したパケット数
	outgoing	DSCP 値ごとに送信したパケット数
CoS	incoming	CoS 値ごとに受信したパケット数
	outgoing	CoS 値ごとに送信したパケット数
Policer	Inprofile	ポリサーごとのプロファイル内パケット数
	OutofProfile	ポリサーごとのプロファイル外パケット数

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) しきい値を設定し、バッファの可用性を確保し、キューセットに対する最大メモリ割り当てを設定します。
mls qos srr-queue input bandwidth	SRR の重みを入力キューに割り当てます。
mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input priority-queue	入力プライオリティ キューを設定し、帯域幅を確保します。
mls qos srr-queue input threshold	WTD しきい値のパーセントを入力キューに割り当てます。

コマンド	説明
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	DSCP 値を出力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングします。
policy-map	ポリシー マップを作成または変更します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対しポートをマッピングします。
srr-queue bandwidth limit	ポートでの最大出力を制限します。
srr-queue bandwidth shape	シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅のシェーピングをイネーブルにします。
srr-queue bandwidth share	共有ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

show mls qos maps

QoS (Quality of Service) マッピング情報を表示するには、**show mls qos maps** ユーザ EXEC コマンドを使用します。分類では、QoS はマッピング テーブルを使用してトラフィックのプライオリティを表示し、受信したサービス クラス (CoS)、Differentiated Service Code Point (DSCP)、または IP precedence 値から対応する CoS または DSCP 値を取得します。

```
show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q |
dscp-mutation dscp-mutation-name | dscp-output-q | ip-prec-dscp | policed-dscp] [ |
{begin | exclude | include} expression]
```

シンタックスの説明

cos-dscp	(任意) CoS/DSCP マップを表示します。
cos-input-q	(任意) CoS 入力キューのしきい値マップを表示します。
cos-output-q	(任意) CoS 出力キューのしきい値マップを表示します。
dscp-cos	(任意) DSCP/CoS マップを表示します。
dscp-input-q	(任意) DSCP 入力キューしきい値マップを表示します。
dscp-mutation <i>dscp-mutation-name</i>	(任意) 指定された DSCP/DSCP-mutation マップを表示します。
dscp-output-q	(任意) DSCP 出力キューしきい値マップを表示します。
ip-prec-dscp	(任意) IP precedence/DSCP マップを表示します。
policed-dscp	(任意) ポリシング設定 DSCP マップを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

ポリシング設定 DSCP、DSCP/CoS、および DSCP/DSCP-mutation マップは、マトリックスとして表示されます。d1 列では、DSCP で最も重要度の高い桁を指定します。d2 行では、DSCP で最も重要度の低い桁を指定します。d1 値および d2 値の共通部分では、ポリシング設定 DSCP、CoS、または Mutated-DSCP 値を提供します。たとえば、DSCP/CoS マップでは、DSCP 値 43 は CoS 値 5 に対応します。

DSCP 入力キューしきい値および DSCP 出力キューしきい値マップは、マトリックスとして表示されます。d1 列では、最も重要度の高い DSCP 番号の桁を指定します。d2 行では、最も重要度の低い DSCP 番号の桁を指定します。d1 値と d2 値の共通部分は、キュー ID およびしきい値 ID を示します。たとえば、DSCP 入力キューしきい値マップでは、DSCP 値 43 はキュー 2 およびしきい値 1 (02-01) に対応することになります。

CoS 入力キューしきい値および CoS 出力キューしきい値マップは、CoS 値を一番上の行、対応するキュー ID およびしきい値 ID は 2 番めの行に表示しています。たとえば、CoS 入力キューしきい値マップでは、CoS 値 5 はキュー 2 およびしきい値 1 (2-1) に対応することになります。

例

次の例では、**show mls qos maps** コマンドの出力を示します。

```
Switch> show mls qos maps
Policed-dscp map:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
  0 : 00 01 02 03 04 05 06 07 08 09
  1 : 10 11 12 13 14 15 16 17 18 19
  2 : 20 21 22 23 24 25 26 27 28 29
  3 : 30 31 32 33 34 35 36 37 38 39
  4 : 40 41 42 43 44 45 46 47 48 49
  5 : 50 51 52 53 54 55 56 57 58 59
  6 : 60 61 62 63

Dscp-cos map:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
  0 : 00 00 00 00 00 00 00 00 01 01
  1 : 01 01 01 01 01 01 02 02 02 02
  2 : 02 02 02 02 03 03 03 03 03 03
  3 : 03 03 04 04 04 04 04 04 04 04
  4 : 05 05 05 05 05 05 05 05 06 06
  5 : 06 06 06 06 06 06 07 07 07 07
  6 : 07 07 07 07

Cos-dscp map:
  cos: 0 1 2 3 4 5 6 7
-----
  dscp: 0 8 16 24 32 40 48 56

IpPrecedence-dscp map:
  ipprec: 0 1 2 3 4 5 6 7
-----
  dscp: 0 8 16 24 32 40 48 56

Dscp-outputq-threshold map:
  d1 :d2 0 1 2 3 4 5 6 7 8 9
-----
  0 : 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
  1 : 02-01 02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01 03-01
  2 : 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
  3 : 03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
  4 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
  5 : 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
  6 : 04-01 04-01 04-01 04-01
```

show mls qos maps

```

Dscp-inputq-threshold map:
d1 :d2  0    1    2    3    4    5    6    7    8    9
-----
0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
2 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01
5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
6 :    01-01 01-01 01-01 01-01

Cos-outputq-threshold map:
      cos:  0    1    2    3    4    5    6    7
-----
queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

Cos-inputq-threshold map:
      cos:  0    1    2    3    4    5    6    7
-----
queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

Dscp-dscp mutation map:
Default DSCP Mutation Map:
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
0 :    00 01 02 03 04 05 06 07 08 09
1 :    10 11 12 13 14 15 16 17 18 19
2 :    20 21 22 23 24 25 26 27 28 29
3 :    30 31 32 33 34 35 36 37 38 39
4 :    40 41 42 43 44 45 46 47 48 49
5 :    50 51 52 53 54 55 56 57 58 59
6 :    60 61 62 63

```

関連コマンド

コマンド	説明
mls qos map	CoS/DSCP マップ、DSCP/CoS マップ、DSCP/DSCP-mutation マップ、IP precedence/DSCP マップ、およびポリシング設定 DSCP マップを定義します。
mls qos srr-queue input cos-map	CoS 値を入力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue input dscp-map	DSCP 値を入力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	DSCP 値を出力キューにマッピング、または DSCP 値をキューおよびしきい値 ID にマッピングします。

show mls qos queue-set

出力キューの QoS (Quality of Service) を表示するには、**show mls qos queue-set** ユーザ EXEC コマンドを使用します。

show mls qos queue-set [*qset-id*] [| **{begin | exclude | include}** *expression*]



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>qset-id</i>	(任意) キューセットの ID です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ~ 2 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mls qos queue-set** コマンドの出力を示します。

```
Switch> show mls qos queue-set
Queueset: 1
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100     200     100     100
threshold2:    100     200     100     100
reserved  :      50      50      50      50
maximum   :     400     400     400     400
Queueset: 2
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100     200     100     100
threshold2:    100     200     100     100
reserved  :      50      50      50      50
maximum   :     400     400     400     400
```

■ show mls qos queue-set

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) しきい値を設定し、バッファの アベイラビリティを保証し、キューセットに対する最大メモ リ割り当てを設定します。

show mls qos vlan

Switch Virtual Interface (SVI) に適用されているポリシー マップを表示するには、**show mls qos vlan** ユーザ EXEC コマンドを使用します。

```
show mls qos vlan vlan-id [ | {begin | exclude | include} expression ]
```

シンタックスの説明	説明
<i>vlan-id</i>	ポリシー マップを表示するために SVI の VLAN ID を指定します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード ユーザ EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **show mls qos vlan** コマンドからの出力は、VLAN ベースの QoS (Quality of Service) がイネーブルでポリシー マップが設定されている場合のみ意味があります。

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 次の例では、**show mls qos vlan** コマンドの出力を示します。

```
Switch> show mls qos vlan 10
Vlan10
Attached policy-map for Ingress:pm-test-pm-2
```

関連コマンド	コマンド	説明
	policy-map	複数のポートに適用できるポリシー マップを作成または変更し、ポリシー マップ コンフィギュレーション モードを開始します。

show monitor

スイッチ上のすべてのスイッチドポートアナライザ (SPAN) セッションおよびリモート SPAN (RSPAN) セッションの情報を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。コマンドにキーワードを指定することで、特定のセッション、すべてのセッション、すべてのローカルセッション、すべてのリモートセッションを表示できます。

```
show monitor [session {session_number | all | local | range list | remote} [detail]] [| {begin
| exclude | include} expression]
```

シンタックスの説明

session	(任意) 指定の SPAN セッションの情報を表示します。
session_number	SPAN または RSPAN のセッション番号を指定します。指定できる範囲は 1 ~ 66 です。
all	すべての SPAN セッションを表示します。
local	ローカルの SPAN セッションのみを表示します。
range list	SPAN セッションの範囲 (<i>list</i> は有効なセッションの範囲) を表示します。1 つのセッション、またはセッション範囲は 2 つの番号で表示され、番号の低いほうを最初に指定します (ハイフンで区切ります)。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。 (注) このキーワードは、特権 EXEC モードの場合のみ使用可能です。
remote	リモートの SPAN セッションのみを表示します。
detail	(任意) 指定のセッションの詳細情報を表示します。
 begin	<i>expression</i> と一致する行から表示を開始します。
 exclude	<i>expression</i> と一致する行を表示から除外します。
 include	指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

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。

```
Switch# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi0/1
Both : Gi0/2-3,Gi0/5-6
Destination Ports : Gi0/20
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。

```
Switch# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi0/1
Both : Gi0/2-3,Gi0/5-6
Destination Ports : Gi0/20
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。

```
Switch# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi0/2
Destination Ports : Gi0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
-----
Type : Local Session
Source Ports :
Both : Gi0/8
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

■ show monitor

関連コマンド

コマンド	説明
monitor session	SPAN または RSPAN セッションを開始、または修正します。

show mvr

現在の Multicast VLAN Registration (MVR) グローバル パラメータ値を表示するには、キーワードを指定しないで **show mvr** 特権 EXEC コマンドを入力します。表示されるのは、MVR がイネーブルであるかどうか、MVR マルチキャスト VLAN、最大クエリ応答時間、マルチキャストグループ数、および MVR モード (dynamic または compatible) です。

```
show mvr [| {begin | exclude | include} expression]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show mvr** コマンドの出力を示します。

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

上記の例では、マルチキャストグループの最大数が 256 に固定されています。MVR モードは、compatible (Catalyst 2900 XL スイッチおよび Catalyst 3500 XL スイッチと連動する場合) または dynamic (動作が IGMP スヌーピング動作と一貫性があり、送信元ポート上でダイナミック MVR メンバシップがサポートされている場合) のいずれかです。

関連コマンド

コマンド	説明
mvr (グローバル コンフィギュレーション)	スイッチ上で MVR をイネーブルにして、設定します。
mvr (インターフェイス コンフィギュレーション)	MVR ポートを設定します。
show mvr interface	コマンドに interface および members キーワードを追加した場合、設定された MVR インターフェイス、指定されたインターフェイスのステータス、またはインターフェイスが属するマルチキャストグループが表示されます。
show mvr members	MVR マルチキャスト グループに属するポートすべてを表示します。グループ内にメンバーがない場合、グループは非アクティブであることを示します。

show mvr interface

Multicast VLAN Registration (MVR) レシーバーおよび送信元ポートを表示するには、キーワードを指定しないで **show mvr interface** 特権 EXEC コマンドを入力します。キーワードを指定してこのコマンドを入力すると、特定のレシーバー ポートの MVR パラメータが表示されます。

```
show mvr interface [interface-id [members [vlan vlan-id]]] [| {begin | exclude | include}
expression]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>interface-id</i>	(任意) インターフェイスの MVR タイプ、ステータス、および即時脱退設定を表示します。 有効なインターフェイスは物理ポート (タイプ、モジュール、ポート番号を含む) を含みます。
members	(任意) 指定されたインターフェイスが属する MVR グループをすべて表示します。
vlan vlan-id	(任意) VLAN 上の MVR グループ メンバーをすべて表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

入力したポートが非 MVR ポートまたは送信元ポートの場合は、エラー メッセージが戻されます。入力したポートがレシーバー ポートの場合は、ポート タイプ、ポート単位のステータス、および即時脱退設定が表示されます。

members キーワードを入力すると、インターフェイス上の MVR グループ メンバーがすべて表示されます。VLAN ID を入力すると、VLAN の MVR グループ メンバーがすべて表示されます。

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

次の例では、**show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface
Port          Type          Status          Immediate Leave
-----
```

■ show mvr interface

```
Gi0/1      SOURCE      ACTIVE/UP      DISABLED
Gi0/2      RECEIVER     ACTIVE/DOWN    DISABLED
```

上記の例にある Status の定義は、次のとおりです。

- ACTIVE は、ポートが VLAN に含まれていることを意味します。
- UP/DOWN は、ポートが転送中か転送中でないかを示します。
- INACTIVE は、ポートが VLAN に含まれていないことを意味します。

次の例では、指定されたインターフェイスの **show mvr interface** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

次の例では、**show mvr interface interface-id members** コマンドの出力を示します。

```
Switch# show mvr interface gigabitethernet0/2 members
239.255.0.0      DYNAMIC ACTIVE
239.255.0.1      DYNAMIC ACTIVE
239.255.0.2      DYNAMIC ACTIVE
239.255.0.3      DYNAMIC ACTIVE
239.255.0.4      DYNAMIC ACTIVE
239.255.0.5      DYNAMIC ACTIVE
239.255.0.6      DYNAMIC ACTIVE
239.255.0.7      DYNAMIC ACTIVE
239.255.0.8      DYNAMIC ACTIVE
239.255.0.9      DYNAMIC ACTIVE
```

関連コマンド

コマンド	説明
mvr (グローバル コンフィギュレーション)	スイッチ上で MVR をイネーブルにして、設定します。
mvr (インターフェイス コンフィギュレーション)	MVR ポートを設定します。
show mvr	スイッチのグローバル MVR 設定を表示します。
show mvr members	MVR マルチキャスト グループに属するすべてのレシーバーポートを表示します。

show mvr members

現在 IP マルチキャスト グループに属するすべてのレシーバーおよび送信元ポートを表示するには、**show mvr members** 特権 EXEC コマンドを使用します。

```
show mvr members [ip-address] [| {begin | exclude | include} expression]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>ip-address</i>	(任意) IP マルチキャスト アドレスです。IP マルチキャスト アドレスを入力すると、マルチキャスト グループに属するすべてのレシーバーおよび送信元ポートが表示されます。IP マルチキャスト アドレスを入力しない場合は、Multicast VLAN Registration (MVR) グループのすべてのメンバーが表示されます。グループ内にメンバーがない場合は、グループは Inactive として表示されます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

show mvr members コマンドは、レシーバーおよび送信元ポートに適用されます。MVR 互換モードの場合、すべての送信元ポートは、すべてのマルチキャスト グループに属します。

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

次の例では、**show mvr members** コマンドの出力を示します。

```
Switch# show mvr members
MVR Group IP      Status      Members
-----
239.255.0.1      ACTIVE      Gi0/1(d), Gi0/5(s)
239.255.0.2      INACTIVE    None
239.255.0.3      INACTIVE    None
239.255.0.4      INACTIVE    None
239.255.0.5      INACTIVE    None
239.255.0.6      INACTIVE    None
239.255.0.7      INACTIVE    None
239.255.0.8      INACTIVE    None
239.255.0.9      INACTIVE    None
```

■ show mvr members

```
239.255.0.10    INACTIVE      None
```

<output truncated>

次の例では、**show mvr members ip-address** コマンドの出力を示します。次のアドレスを持った IP マルチキャスト グループのメンバーを表示します。

```
Switch# show mvr members 239.255.0.2
239.255.003.--22    ACTIVE      Gi0/1 (d), Gi0/2 (d), Gi0/3 (d),
                  Gi0/4 (d), Gi0/5 (s)
```

関連コマンド

コマンド	説明
mvr (グローバル コンフィギュレーション)	スイッチ上で MVR をイネーブルにして、設定します。
mvr (インターフェイス コンフィギュレーション)	MVR ポートを設定します。
show mvr	スイッチのグローバル MVR 設定を表示します。
show mvr interface	コマンドに members キーワードを追加した場合、設定された MVR インターフェイス、指定されたインターフェイスのステータス、またはインターフェイスが属するマルチキャスト グループが表示されます。

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、**show network policy profile** 特権 EXEC コマンドを使用します。

```
show network-policy profile [profile number] [detail] [| {begin | exclude | include}
expression]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<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と、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。
<i>detail</i>	(任意) 詳細なステータスと統計情報を表示します。
<i>begin</i>	(任意) <i>expression</i> と一致する行から表示を開始します。
<i>exclude</i>	(任意) <i>expression</i> と一致する行を表示から除外します。
<i>include</i>	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、**show network-policy profile** コマンドの出力を示します。

```
Switch# 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 network-policy profile

関連コマンド

コマンド	説明
network-policy	インターフェイスにネットワーク ポリシーを適用します。
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ます。
network-policy profile (ネット ワーク ポリシー コンフィギュレ ーション)	ネットワーク ポリシー プロファイルの属性を設定します。

show nmosp

スイッチのネットワーク モビリティ サービス プロトコル (NMSP) 情報を表示するには、**show nmosp** 特権 EXEC コマンドを入力します。このコマンドを使用できるのは、スイッチで暗号化ソフトウェア イメージが実行されている場合だけです。

```
show nmosp {attachment suppress interface | capability | notification interval | statistics
             {connection | summary} | status | subscription {detail | summary}} [| {begin | exclude
             | include} expression]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

attachment suppress interface	接続抑制インターフェイスを表示します。
capability	サポートされているサービスとサブサービスなどのスイッチ機能を表示します。
notification interval	サポートされているサービスの通知間隔を表示します。
statistics {connection summary}	NMSP 統計情報を表示します。 <ul style="list-style-type: none"> • connection : 接続ごとにメッセージカウンタを表示します。 • summary : グローバル カウンタを表示します。
status	NMSP 接続に関する情報を表示します。
subscription {detail summary}	NMSP 接続ごとにサブスクリプション情報を表示します。 <ul style="list-style-type: none"> • detail : 接続ごとにサブスクライブされたサービスとサブサービスをすべて表示します。 • summary : 接続ごとにサブスクライブされたサービスをすべて表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

例

次の例では、**show nmosp attachment suppress interface** コマンドの出力を示します。

```
Switch# show nmosp attachment suppress interface
NMSP Attachment Suppression Interfaces
-----
GigabitEthernet1/1
```

GigabitEthernet1/2

次の例では、**show nmosp capability** コマンドの出力を示します。

```
Switch# show nmosp capability
NMSP Switch Capability
-----
Service          Subservice
-----
Attachment      Wired Station
Location        Subscription
```

次の例では、**show nmosp notification interval** コマンドの出力を示します。

```
Switch# show nmosp notification interval
NMSP Notification Intervals
-----
Attachment notify interval: 30 sec (default)
Location notify interval: 30 sec (default)
```

次の例では、**show nmosp statistics connection** コマンドと **show nmosp statistics summary** コマンドの出力を示します。

```
Switch# show nmosp statistics connection
NMSP Connection Counters
-----
Connection 1:
  Connection status: UP
  Freed connection: 0

  Tx message count      Rx message count
  -----
  Subscr Resp: 1        Subscr Req: 1
  Capa Notif: 1         Capa Notif: 1
  Atta Resp: 1          Atta Req: 1
  Atta Notif: 0
  Loc Resp: 1           Loc Req: 1
  Loc Notif: 0
  Unsupported msg: 0

Switch# show nmosp statistics summary
NMSP Global Counters
-----
  Send too big msg: 0
  Failed socket write: 0
  Partial socket write: 0
  Socket write would block: 0
  Failed socket read: 0
  Socket read would block: 0
  Transmit Q full: 0
  Max Location Notify Msg: 0
  Max Attachment Notify Msg: 0
  Max Tx Q Size: 0
```

次の例では、**show nmosp status** コマンドの出力を示します。

```
Switch# show nmosp status
NMSP Status
-----
NMSP: enabled
MSE IP Address      TxEchoResp RxEchoReq TxData RxData
172.19.35.109      5 5 4 4
```

次の例では、**show nmsp show subscription detail** コマンドと **show nmsp show subscription summary** コマンドの出力を示します。

```
Switch# show nmsp subscription detail
Mobility Services Subscribed by 172.19.35.109:
Services                Subservices
-----                -
Attachment:            Wired Station
Location:              Subscription
```

```
Switch# show nmsp subscription summary
Mobility Services Subscribed:
MSE IP Address         Services
-----                -
172.19.35.109         Attachment, Location
```

関連コマンド

コマンド	説明
clear nmsp statistics	NMSP 統計カウンタをクリアします。
nmsp	スイッチ上で Network Mobility Services Protocol (NMSP) をイネーブルにします。

show pagp

ポート集約プロトコル (PAgP) チャンネル グループ情報を表示するには、**show pagp** ユーザ EXEC コマンドを使用します。

```
show pagp [channel-group-number] {counters | dual-active | internal | neighbor} [| {begin
| exclude | include} expression]]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>channel-group-number</i>	(任意) チャンネル グループの番号です。指定できる範囲は 1 ~ 6 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 ステータスを表示します。
internal	内部情報を表示します。
neighbor	ネイバー情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(46)SE	dual-active キーワードが追加されました。

使用上のガイドライン

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。

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

次の例では、**show pagp 1 counters** コマンドの出力を示します。

```
Switch> show pagp 1 counters
          Information          Flush
Port      Sent   Recv   Sent   Recv
-----
Channel group: 1
Gi0/1     45    42     0     0
Gi0/2     45    41     0     0
```


次の例では、**show pagp 1 internal** コマンドの出力を示します。

```
Switch> 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  Partner  PAgP    Learning  Group
Gi0/1         SC   U6/S7  H       30s    1        128     Any       16
Gi0/2         SC   U6/S7  H       30s    1        128     Any       16
```

次の例では、**show pagp 1 neighbor** コマンドの出力を示します。

```
Switch> 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          Partner          Partner          Partner Group
Name          Device ID       Port             Age  Flags  Cap.
Gi0/1         switch-p2       0002.4b29.4600  Gi0/1           9s SC   10001
Gi0/2         switch-p2       0002.4b29.4600  Gi0/2           24s SC  10001
```

次の例では、**show pagp dual-active** コマンドの出力を示します。

```
Switch> 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           Device ID       Port     Version
Gi0/1         No           Switch          0002.4b29.4600  Gi0/3   N/A
Gi0/2         No           Switch          0002.4b29.4600  Gi0/4   N/A

<output truncated>
```

関連コマンド

コマンド	説明
clear pagp	PAgP チャネル グループ情報をクリアします。

show parser macro

スイッチ上のすべての設定済マクロまたは 1 つのマクロのパラメータを表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。

```
show parser macro [{brief | description [interface interface-id] | name macro-name}]
                  [| {begin | exclude | include} expression]
```

シンタックスの説明

brief	(任意) 各マクロの名前を表示します。
description [interface interface-id]	(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 macro-name	(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。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show parser macro** コマンドの出力を示します。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。

```
Switch# 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

<テキスト出力は省略>

-----
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
```

<テキスト出力は省略>

```
-----  
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
```

<テキスト出力は省略>

```
-----  
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
```

<テキスト出力は省略>

```
-----  
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
```

<テキスト出力は省略>

```
-----  
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
```

次の例では、**show parser macro name** コマンドの出力を示します。

```
Switch# 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
```

次の例では、**show parser macro brief** コマンドの出力を示します。

```
Switch# 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
```

次の例では、**show parser macro description** コマンドの出力を示します。

```
Switch# show parser macro description
Global Macro(s): cisco-global
Interface      Macro Description(s)
-----
Gi0/1          standard-switch10
Gi0/2          this is test macro
-----
```

次の例では、**show parser description interface** コマンドの出力を示します。

```
Switch# show parser macro description interface gigabitethernet0/2
Interface      Macro Description
-----
Gi0/2          this is test macro
-----
```

関連コマンド

コマンド	説明
macro apply	インターフェイス上にマクロを適用するか、インターフェイス上にマクロを適用して追跡します。
macro description	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追加します。
macro global	スイッチ上にマクロを適用するか、スイッチ上にマクロを適用して追跡します。
macro global description	スイッチに適用されたマクロについての説明を追加します。
macro name	マクロを作成します。
show running-config	定義されたマクロを含む現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。

show policy-map

着信トラフィックの分類基準を定義する QoS (Quality of Service) ポリシー マップを表示するには、**show policy-map** ユーザ EXEC コマンドを使用します。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。

```
show policy-map [policy-map-name [class class-map-name]] [| {begin | exclude | include}
expression]
```



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>policy-map-name</i>	(任意) 指定されたポリシーマップの名前を表示します。
class <i>class-map-name</i>	(任意) 各クラスの QoS ポリシー アクションを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注) **control-plane** および **interface** 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せんが、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。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show policy-map** コマンドの出力を示します。

```
Switch> show policy-map
Policy Map videowizard_policy2
  class videowizard_10-10-10-10
    set dscp 34
    police 100000000 2000000 exceed-action drop

Policy Map mypolicy
  class dscp5
    set dscp 6
```

■ show policy-map

関連コマンド

コマンド	説明
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー マップを作成または変更します。

show port-security

インターフェイスまたはスイッチのポート セキュリティ設定を表示するには、**show port-security** 特権 EXEC コマンドを使用します。

```
show port-security [interface interface-id] [address | vlan] [| {begin | exclude | include}
expression]
```

シンタックスの説明

interface interface-id	(任意) 指定されたインターフェイスのポート セキュリティ設定を表示します。有効なインターフェイスは物理ポート (タイプ、モジュール、ポート番号を含む) を含みます。
address	(任意) すべてのポートまたは指定されたポート上のすべてのセキュア MAC (メディア アクセス制御) アドレスを表示します。
vlan	(任意) 指定されたインターフェイスのすべての VLAN のポート セキュリティ設定を表示します。このキーワードは、スイッチポート モードが trunk に設定されているインターフェイス上でのみ表示されます。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

キーワードを指定しないでこのコマンドを入力すると、スイッチのすべてのセキュア ポートの管理ステータスおよび動作ステータスが出力されます。

interface-id を入力した場合、コマンドはインターフェイスのポート セキュリティ設定を表示します。

address キーワードを指定してコマンドを入力すると、すべてのインターフェイスのセキュア MAC アドレス、および各セキュア アドレスのエージング情報が表示されます。

interface-id キーワードおよび **address** キーワードを指定してコマンドを入力すると、各セキュア アドレスのエージング情報を持ったインターフェイスの MAC アドレスがすべて表示されます。インターフェイス上でポート セキュリティがイネーブルでない場合も、このコマンドを使用して、そのインターフェイスの MAC アドレスをすべて表示できます。

vlan キーワードを指定してコマンドを入力すると、インターフェイスの VLAN すべてに対するセキュア MAC アドレスの最大設定数および現在数が表示されます。このオプションは、スイッチポートモードが **trunk** に設定されているインターフェイス上でのみ表示されます。

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。

show port-security

例 次の例では、**show port-security** コマンドの出力を示します。

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)      (Count)
-----
      Gi0/1          1              0              0              Shutdown
-----
Total Addresses in System (excluding one mac per port)      : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

次の例では、**show port-security interface interface-id** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet0/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

次の例では、**show port-security address** コマンドの出力を示します。

```
Switch# show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1    0006.0700.0800  SecureConfigured   Gi0/2    1
-----
Total Addresses in System (excluding one mac per port)      : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

次の例では、**show port-security interface gigabitethernet0/2 address** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet0/2 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1    0006.0700.0800  SecureConfigured   Gi0/2    1
-----
Total Addresses: 1
```

次の例では、**show port-security interface interface-id vlan** コマンドの出力を示します。

```
Switch# show port-security interface gigabitethernet0/2 vlan
Default maximum: not set, using 5120
VLAN  Maximum  Current
   5    default   1
  10    default   54
  11    default  101
  12    default  101
  13    default  201
  14    default  501
```


関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからスイッチ上またはインターフェイス上の特定のタイプのセキュア アドレスまたはすべてのセキュア アドレスを削除します。
switchport port-security	ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。

show power inline

指定された Power over Ethernet (PoE) ポートまたはすべての PoE ポートの PoE ステータスを表示するには、**show power inline** ユーザ EXEC コマンドを使用します。

```
show power inline [police] [interface-id | consumption] [| {begin | exclude | include}
expression]
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

police	(任意) リアルタイム電力消費に関する電力ポリシー情報を表示します。
<i>interface-id</i>	(任意) 指定されたインターフェイスの PoE 関連電力管理情報を表示します。
consumption	(任意) PoE ポートに接続した装置に割り当てられた電力を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。
12.2(46)SE	police キーワードが追加されました。

使用上のガイドライン

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

次の例では、**show power inline** コマンドの出力を示します。出力では、ポート 2 がスタティックに設定されており、電力がこのポートに事前に割り当てられていますが、受電装置は接続されていません。ポート 6 は、最大ワット数が 10 W に設定されているために **power-deny** ステートになっているスタティック ポートです。接続された受電装置には、Class 0 または Class 3 装置に対して報告されたクラス の最大ワット数が設定されています。表 2-32 に、出力フィールドの説明を示します。

```
Switch> show power inline
Available:370.0(w) Used:80.6(w) Remaining:289.4(w)
```

Interface	Admin	Oper	Power (Watts)	Device	Class	Max
Fa0/1	auto	on	6.3	IP Phone 7910	n/a	15.4
Fa0/2	static	off	15.4	n/a	n/a	15.4
Fa0/3	auto	on	6.3	IP Phone 7910	n/a	15.4
Fa0/4	auto	on	6.3	IP Phone 7960	2	15.4

```

Fa0/5    static on          15.4    IP Phone 7960    2    15.4
Fa0/6    static power-deny 10.0    n/a            n/a    10.0
Fa0/7    auto on             6.3     IP Phone 7910    n/a    15.4
<テキスト出力は省略>

```

次の例では、ポートに対する **show power inline** コマンドの出力を示します。

```

Switch> show power inline fastethernet0/1
Interface Admin Oper      Power Device          Class Max
              (Watts)
-----
Fa0/1      auto  on       6.3   IP Phone 7910      n/a   15.4

```

次の例では、すべての PoE スイッチ ポートの **show power inline consumption** コマンドの出力を示します。

```

Switch> show power inline consumption
Default PD consumption : 15400 mW

```

表 2-32 show power inline interface のフィールドの説明

フィールド	説明
Admin	管理モード : auto、off、static
Oper	動作モード : <ul style="list-style-type: none"> on : 受電装置が検出され、電力が適用されています。 off : PoE が適用されていません。 faulty : 装置検出または受電装置が障害の状態です。 power-deny : 受電装置が検出されていますが、PoE が使用できない状態か、最大ワット数が検出された受電装置の最大数を超えています。
Power	PoE の供給ワット数
Device	検出された装置のタイプ : n/a、unknown、Cisco powered-device、IEEE powered-device、<CDP からの名前>
Class	IEEE 分類 : n/a、Class <0 ~ 4>
Available	システム内の PoE の総数
Used	ポートに割り当てられている PoE の数
Remaining	システム内でポートに割り当てられていない PoE の数 (Available – Used = Remaining)

次の例では、スイッチに対する **show power inline police** コマンドの出力を示します。表 2-33 に、出力フィールドの説明を示します。

```

Switch> show power inline police
Module  Available  Used  Remaining
         (Watts)  (Watts)  (Watts)
-----
1        370.0      0.0     370.0
3        865.0     864.0     1.0

Admin Oper      Admin Oper      Cutoff Oper
Interface State State      Police  Police      Power  Power
-----
Gi0/1  auto  off       none    n/a        n/a    0.0
Gi0/2  auto  off       log     n/a        5.4    0.0
Gi0/3  auto  off       errdisable n/a        5.4    0.0
Gi0/4  off   off       none    n/a        n/a    0.0

```

show power inline

```

Gi0/5  off  off      log      n/a      5.4  0.0
Gi0/6  off  off      errdisable n/a      5.4  0.0
Gi0/7  auto  off      none     n/a      n/a   0.0
Gi0/8  auto  off      log      n/a      5.4  0.0
Gi0/9  auto  on       none     n/a      n/a   5.1
Gi0/10 auto  on       log      ok       5.4  4.2
Gi0/11 auto  on       log      log      5.4  5.9
Gi0/12 auto  on       errdisable ok       5.4  4.2
Gi0/13 auto  errdisable n/a      5.4  0.0

```

<テキスト出力は省略>

上の例では、次のようになっています。

- Gi0/1 ポートはシャットダウンされ、ポリシングは設定されていません。
- Gi0/2 ポートはシャットダウンされますが、ポリシングはイネーブルです。ポリシングアクションによって Syslog メッセージが生成されます。
- Gi0/3 ポートはシャットダウンされますが、ポリシングはイネーブルです。ポリシングアクションによってポートがシャットダウンされます。
- Gi0/4 ポートでは、装置検出がディセーブルで、ポートに電力は適用されず、ポリシングがディセーブルになっています。
- Gi0/5 ポートでは、装置検出がディセーブルで、電力はポートに適用されませんが、ポリシングがイネーブルになっています。ポリシングアクションによって Syslog メッセージが生成されます。
- Gi0/6 ポートでは、装置検出がディセーブルで、電力はポートに適用されませんが、ポリシングがイネーブルになっています。ポリシングアクションによってポートがシャットダウンされます。
- Gi0/7 ポートは起動していてポリシングはディセーブルですが、スイッチは接続装置に電力を供給しません。
- Gi0/8 ポートは起動していて、ポリシングがイネーブルになっています。ポリシングアクションによって Syslog メッセージが生成されます。スイッチは受電装置に電力を供給しません。
- Gi0/9 ポートは起動していて、受電装置に接続され、ポリシングはディセーブルになっています。
- Gi0/10 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによって Syslog メッセージが生成されます。リアルタイム電力消費がカットオフ値より少ないため、ポリシングアクションは作動しません。
- Gi0/11 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによって Syslog メッセージが生成されます。
- Gi0/12 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによってポートはシャットダウンされます。リアルタイム電力消費がカットオフ値より少ないため、ポリシングアクションは作動しません。
- Gi0/13 ポートは起動していて、受電装置に接続され、ポリシングがイネーブルになっています。ポリシングアクションによってポートはシャットダウンされます。

次の例では、スイッチに対する **show power inline police interface-id** コマンドの出力を示します。表 2-33 に、出力フィールドの説明を示します。

```

Switch> show power inline police gigabitethernet0/4
Interface Admin Oper      Admin      Oper      Cutoff Oper
          State State      Police     Police     Power  Power
-----
Gi0/4    auto  power-deny log         n/a       4.0    0.0

```

表 2-33 show power inline police のフィールドの説明

フィールド	説明
Available	スイッチでの設定電力の合計で、ワット数 (W) です。
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計 (ワット数) です。(Available - Used = Remaining)
Admin State	管理モード : auto、off、static
Oper State	動作モード : <ul style="list-style-type: none"> errdisable : ポリシングはイネーブルです。 faulty : 受電装置での装置検出が障害の状態です。 off : PoE が適用されていません。 on : 受電装置が検出され、電力が適用されています。 power-deny : 受電装置が検出されていますが、PoE が使用できない状態か、リアルタイム電力消費が最大電力割り当てを超えています。 <p>(注) 動作モードは、指定した PoE ポートまたはスイッチのすべての PoE ポートの現在の PoE ステートです。</p>
Admin Police	リアルタイム電力消費ポリシング機能のステータス : <ul style="list-style-type: none"> errdisable : ポリシングがイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチはポートをシャットダウンします。 log : ポリシングはイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチが Syslog メッセージを生成します。 none : ポリシングはディセーブルです。
Oper Police	ポリシング ステータス : <ul style="list-style-type: none"> errdisable : リアルタイム電力消費が最大電力割り当てを超えています。スイッチが PoE ポートをシャットダウンします。 log : リアルタイム電力消費が最大電力割り当てを超えています。スイッチが Syslog メッセージを生成します。 n/a : 装置検出がディセーブルで、電力が PoE ポートに適用されていないか、ポリシングアクションが設定されていません。 ok : リアルタイム電力消費が最大電力割り当てより少ない状態です。
Cutoff Power	ポートに割り当てられている最大電力です。リアルタイム電力消費がこの値を上回ると、スイッチは設定されたポリシングアクションを実行します。
Oper Power	受電装置のリアルタイム電力消費です。

関連コマンド

コマンド	説明
logging event power-inline-status	PoE イベントのロギングをイネーブルにします。
power inline	指定した PoE ポートまたはすべての PoE ポートの電力管理モードを設定します。
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。

show sdm prefer

特定の機能に対するシステム リソースの割り当てを最大化するために使用可能な Switch Database Management (SDM) テンプレートに関する情報を表示するには、**show sdm prefer** 特権 EXEC コマンドを使用します。

```
show sdm prefer [default | dual-ipv4-and-ipv6 default | qos] [| {begin | exclude | include}
expression]
```

シンタックスの説明

default	(任意) 機能間のシステム リソースのバランスをとるテンプレートを表示します。
dual-ipv4-and-ipv6 default	(注) (任意) IPv4 と IPv6 の両方をサポートするデュアル テンプレートを表示します。
qos	(任意) QoS (Quality of Service) アクセス コントロール エントリ (ACE) 用のシステム リソースを最大化するテンプレートを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(40)SE	dual-ipv4-and-ipv6 default キーワードが追加されました。

使用上のガイドライン

sdm prefer グローバル コンフィギュレーション コマンドを使用し、SDM テンプレートを変更した場合は、設定の変更を有効にするためスイッチをリロードする必要があります。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになる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。

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 次の例では、**show sdm prefer** コマンドの出力例を示します。

```
Switch# show sdm prefer default
"default" template:
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

number of unicast mac addresses:                8K
```

```
number of IPv4 IGMP groups:          256
number of IPv4/MAC qos aces:         128
number of IPv4/MAC security aces:    384
```

次の例では、**show sdm prefer qos** コマンドの出力例を示します。

```
Switch# show sdm prefer qos
"qos" template:
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

number of unicast mac addresses:      8K
number of IPv4 IGMP groups:          256
number of IPv4/MAC qos aces:         384
number of IPv4/MAC security aces:    128
```

関連コマンド

コマンド	説明
sdm prefer	SDM テンプレートを最大化されたリソース量に設定します。

show setup express

Express Setup モードがスイッチでアクティブかどうかを表示するには、**show setup express** 特権 EXEC コマンドを使用します。

```
show setup express [ | {begin | exclude | include} expression]
```

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例は、**show setup express** コマンドの出力を示しています。

```
Switch# show setup express
express setup mode is active
```

関連コマンド

コマンド	説明
setup express	Express Setup モードをイネーブルにします。

show shell

シェル情報を表示するには、**show shell** 特権 EXEC コマンドを使用します。

show shell [**environment** | **functions** | **triggers**] [| **{begin | exclude | include}**] *expression*

シンタックスの説明

environment	(任意) シェル環境情報を表示します。
functions	(任意) マクロ情報を表示します。
triggers	(任意) イベント トリガー情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

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。

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

次の例では、**show shell triggers** 特権 EXEC 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。

```
Switch# show shell triggers

User defined triggers
-----
Built-in triggers
-----
Trigger Id: CISCO_PHONE_EVENT
Trigger description: Event for ip-phone macro
Trigger environment: ACCESS_VLAN=1 VOICE_VLAN=2
Trigger mapping function: CISCO_PHONE_AUTO_SMARTPORT

Trigger Id: CISCO_ROUTER_EVENT
Trigger description: Event for router macro
Trigger environment: NATIVE_VLAN=1
Trigger mapping function: CISCO_ROUTER_AUTO_SMARTPORT

Trigger Id: CISCO_SWITCH_EVENT
Trigger description: Event for switch macro
Trigger environment: NATIVE_VLAN=1
Trigger mapping function: CISCO_SWITCH_AUTO_SMARTPORT
```

```

Trigger Id: CISCO_WIRELESS_AP_EVENT
Trigger description: Event for Wireless Access Point macro
Trigger environment: NATIVE_VLAN=1
Trigger mapping function: CISCO_AP_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
Trigger description: Event for Wireless Lightweight Access Point macro
Trigger environment: NATIVE_VLAN=1
Trigger mapping function: CISCO_LWAP_AUTO_SMARTPORT

```

次の例では、**show shell functions** 特権 EXEC 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。

```

Switch# show shell functions
#User defined functions:

#Built-in functions:
function CISCO_AP_AUTO_SMARTPORT () {
    if [[ $LINKUP -eq 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
            exit
        end
    fi
    if [[ $LINKUP -eq 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
                if [[ $AUTH_ENABLED -eq NO ]]; then
                    no switchport mode
                    no switchport trunk encapsulation
                fi
            fi
        exit
    end
fi
}

function CISCO_SWITCH_AUTO_SMARTPORT () {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface $INTERFACE
                macro description $TRIGGER
                auto qos voip trust
                switchport trunk encapsulation dot1q
                switchport trunk native vlan $NATIVE_VLAN
                switchport trunk allowed vlan ALL
                switchport mode trunk
            exit
        end
    else
        conf t

```

```
        interface $INTERFACE
            no macro description
            no auto qos voip trust
            no switchport mode trunk
            no switchport trunk encapsulation dot1q
            no switchport trunk native vlan $NATIVE_VLAN
            no switchport trunk allowed vlan ALL
        exit
    end
fi
}
```

<テキスト出力は省略>

関連コマンド

コマンド	説明
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto execute	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。
shell trigger	イベント トリガーを作成します。

show spanning-tree

スパニングツリー状態情報を表示するには、**show spanning-tree** ユーザ EXEC コマンドを使用します。

```
show spanning-tree [bridge-group | active [detail] | backbonefast | blockedports | bridge |
detail [active] | inconsistentports | interface interface-id | mst | pathcost method | root
| summary [totals] | uplinkfast | vlan vlan-id] [ | {begin | exclude | include} expression]
```

```
show spanning-tree bridge-group [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree {vlan vlan-id | bridge-group} bridge [address | detail | forward-time
| hello-time | id | max-age | priority [system-id] | protocol] [ | {begin | exclude |
include} expression]
```

```
show spanning-tree {vlan vlan-id | bridge-group} root [address | cost | detail |
forward-time | hello-time | id | max-age | port | priority [system-id] [ | {begin |
exclude | include} expression]
```

```
show spanning-tree interface interface-id [active [detail] | cost | detail [active] |
inconsistency | portfast | priority | rootcost | state] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree mst [configuration [digest]] | [instance-id [detail | interface interface-id
| detail]] [ | {begin | exclude | include} expression]
```

シンタックスの説明

<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 [detail]	(任意) アクティブ インターフェイスのスパニングツリー情報のみを表示します (特権 EXEC モードの場合のみ使用可能)。
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の情報を表示します (特権 EXEC モードの場合のみ使用可能)。
bridge [address detail forward-time hello-time id max-age priority [system-id] protocol]	(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 (オプションのキーワードは特権 EXEC モードの場合のみ使用可能)。
detail [active]	(任意) インターフェイス情報の詳細サマリーを表示します (active キーワードは特権 EXEC モードの場合のみ使用可能)。
inconsistentports	(任意) 矛盾するポートの情報を表示します (特権 EXEC モードの場合のみ使用可能)。

interface <i>interface-id</i> [active [detail] cost detail [active] inconsistency portfast priority rootcost state]	(任意) 指定されたインターフェイスのスパニングツリー情報を表示します (portfast および state 以外のすべてのオプションは特権 EXEC モードでのみ使用可能)。各インターフェイスは、スペースで区切って入力します。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としては、物理ポート、VLAN、およびポート チャネルがあります。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範囲は 1 ~ 6 です。
mst [configuration digest] [<i>instance-id</i> detail interface <i>interface-id</i> [detail]]	(任意) Multiple Spanning-Tree (MST) のリージョン設定およびステータスを表示します (特権 EXEC モードの場合のみ使用可能)。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • digest : (任意) 現在の MST 設定 ID (MSTCI) に含まれる MD5 ダイジェストを表示します。1 つは標準スイッチ、もう 1 つは先行標準スイッチ用の 2 つの別個ダイジェストが表示されます (特権 EXEC モードの場合のみ使用可能)。 IEEE 標準の実装のために専門用語が更新され、<i>txholdcount</i> フィールドが追加されました。 境界ポート用に新しいマスター ロールが表示されます。 IEEE 標準ブリッジがポートに先行標準ブリッジプロトコルデータユニット (BPDU) を送信した場合、<i>pre-standard</i> または <i>Pre-STD</i> という用語が表示されます。 ポートが先行標準 BPDU を送信するように設定され、ポートで先行標準 BPDU が受信されなかったとき、<i>pre-standard (config)</i> または <i>Pre-STD-Cf</i> という用語が表示されます。 先行標準 BPDU を送信するように設定されていないポートで先行標準 BPDU が受信された場合、<i>pre-standard (rcvd)</i> または <i>Pre-STD-Rx</i> という用語が表示されます。 下位指定情報が指定ポートで受信された場合、指定ポートがフォワーディング ステートに戻るか指定が中止されるまで、<i>dispute</i> フラグが表示されます。 • instance-id : 1 つのインスタンス ID、それぞれをハイフンで区切った ID の範囲、またはカンマで区切った一連の ID を指定することができます。指定できる範囲は 1 ~ 4094 です。現在設定されているインスタンスの数が表示されます。 • interface interface-id : (任意) 有効なインターフェイスとしては、物理ポート、VLAN、およびポート チャネルがあります。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範囲は 1 ~ 6 です。 • detail : (任意) インスタンスまたはインターフェイスの詳細情報を表示します。
pathcost method	(任意) デフォルトのパス コスト方式を表示します (特権 EXEC モードの場合のみ使用可能)。
root [address cost detail forward-time hello-time id max-age port priority [system-id]]	(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 (すべてのキーワードが特権 EXEC モードの場合のみ使用可能)。

show spanning-tree

summary [totals]	(任意) ポート状態のサマリー、またはスパニングツリー ステート セクションの総行数を表示します。 <i>IEEE Standard</i> という語は、スイッチ上で実行されている MST バージョンを識別します。
uplinkfast	(任意) スパニングツリー UplinkFast ステータスを表示します。
vlan vlan-id [active [detail] backbonefast blockedports bridge [address detail] forward-time hello-time id max-age priority [system-id] protocol]	(任意) 指定された VLAN のスパニングツリー情報を表示します (キーワードの一部は特権 EXEC モードの場合のみ使用可能)。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	digest キーワードが追加され、新規ダイジェストおよび伝送ホールドカウンタフィールドが表示されます。

使用上のガイドライン

vlan-id 変数を省略した場合は、すべての VLAN のスパニングツリー インスタンスにコマンドが適用されます。

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

次の例では、**show spanning-tree active** コマンドの出力を示します。

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost        3038
             Port        24 (GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153 (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface          Role Sts Cost          Prio.Nbr Type
-----
Gi0/1              Root FWD 3019         128.24  P2p
```

<output truncated>

次の例では、**show spanning-tree detail** コマンドの出力を示します。

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 1 (GigabitEthernet0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  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
  Uplinkfast enabled

Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
  Port path cost 3019, Port priority 128, Port Identifier 128.24.
  Designated root has priority 32768, address 0001.42e2.cdd0
  Designated bridge has priority 32768, address 00d0.bbf5.c680
  Designated port id is 128.25, designated path cost 19
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 0, received 72364
<output truncated>
```

次の例では、**show spanning-tree interface interface-id** コマンドの出力を示します。

```
Switch# show spanning-tree interface gigabitethernet0/1
Vlan          Role Sts Cost      Prio.Nbr Type
-----
VLAN0001      Root FWD 3019      128.24  P2p

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short

Name          Blocking Listening Learning Forwarding STP Active
-----
VLAN0001      1          0          0          11         12
VLAN0002      3          0          0          1          4
VLAN0004      3          0          0          1          4
VLAN0006      3          0          0          1          4
VLAN0031      3          0          0          1          4
VLAN0032      3          0          0          1          4
<output truncated>

-----
37 vlans          109      0          0          47         156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----
Number of transitions via uplinkFast (all VLANs)          : 0
```

show spanning-tree

```

Number of proxy multicast addresses transmitted (all VLANs) : 0

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs)           : 0
Number of inferior BPDUs received (all VLANs)              : 0
Number of RLQ request PDUs received (all VLANs)            : 0
Number of RLQ response PDUs received (all VLANs)           : 0
Number of RLQ request PDUs sent (all VLANs)                : 0
Number of RLQ response PDUs sent (all VLANs)               : 0

```

次の例では、**show spanning-tree mst configuration** コマンドの出力を示します。

```

Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0         1-9,21-4094
1         10-20
-----

```

次の例では、**show spanning-tree mst interface interface-id** コマンドの出力を示します。

```

Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (STP) bpdu guard : disable (default)
Bpdus sent 5, received 74

Instance role state cost prio vlans mapped
0 root FWD 200000 128 1,12,14-4094

```

次の例では、**show spanning-tree mst 0** コマンドの出力を示します。

```

Switch# show spanning-tree mst 0
##### MST00 vlans mapped: 1-9,21-4094
Bridge address 0002.4b29.7a00 priority 32768 (32768 sysid 0)
Root address 0001.4297.e000 priority 32768 (32768 sysid 0)
      port Gi0/1 path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured hello time 2, forward delay 15, max age 20, max hops 20

Interface          role state cost prio type
-----
GigabitEthernet0/1 root FWD 200000 128 P2P bound(STP)
GigabitEthernet0/2 desg FWD 200000 128 P2P bound(STP)
Port-channel1      desg FWD 200000 128 P2P bound(STP)

```

関連コマンド

コマンド	説明
clear spanning-tree counters	スパンニングツリーのカウンタをクリアします。
clear spanning-tree detected-protocols	プロトコル移行プロセスを再開します。
spanning-tree backbonefast	BackboneFast 機能をイネーブルにします。
spanning-tree bpdudfilter	インターフェイスでのブリッジプロトコルデータユニット (BPDU) の送受信を禁止します。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。

コマンド	説明
<code>spanning-tree cost</code>	スパニングツリーの計算に使用するパス コストを設定します。
<code>spanning-tree extend system-id</code>	拡張システム ID 機能をイネーブルにします。
<code>spanning-tree guard</code>	選択されたインターフェイスに対応するすべての VLAN に対して、ルート ガード機能またはループ ガード機能をイネーブルにします。
<code>spanning-tree link-type</code>	スパニングツリーがフォワーディング ステートに高速移行するように、デフォルトリンクタイプ設定を上書きします。
<code>spanning-tree loopguard default</code>	単一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ないようにします。
<code>spanning-tree mst configuration</code>	Multiple Spanning-Tree (MST) リージョンを設定するための MST コンフィギュレーション モードを開始します。
<code>spanning-tree mst cost</code>	MST の計算に使用するパス コストを設定します。
<code>spanning-tree mst forward-time</code>	すべての MST インスタンスについて転送遅延時間を設定します。
<code>spanning-tree mst hello-time</code>	ルート スイッチ コンフィギュレーションメッセージが送信する hello BPDU の間隔を設定します。
<code>spanning-tree mst max-age</code>	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。
<code>spanning-tree mst max-hops</code>	BPDU をドロップしてインターフェイス用に保持していた情報を期限切れにするまでの、MST リージョンでのホップ数を設定します。
<code>spanning-tree mst port-priority</code>	インターフェイス プライオリティを設定します。
<code>spanning-tree mst priority</code>	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。
<code>spanning-tree mst root</code>	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
<code>spanning-tree port-priority</code>	インターフェイス プライオリティを設定します。
<code>spanning-tree portfast</code> (グローバル コンフィギュレーション)	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
<code>spanning-tree portfast</code> (インターフェイス コンフィギュレーション)	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。
<code>spanning-tree uplinkfast</code>	リンクまたはスイッチに障害がある場合、またはスパニング ツリーが自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにします。
<code>spanning-tree vlan</code>	VLAN 単位でスパニング ツリーを設定します。

show storm-control

スイッチまたは指定のインターフェイス上で、ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御の設定を表示したり、ストーム制御履歴を表示したりするには、**show storm-control** ユーザ EXEC コマンドを使用します。

```
show storm-control [interface-id] [broadcast | multicast | unicast] [ | {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) 物理ポートのインターフェイス ID (タイプ、モジュール、ポート番号を含む)
broadcast	(任意) ブロードキャスト ストームしきい値設定を表示します。
multicast	(任意) マルチキャスト ストームしきい値設定を表示します。
unicast	(任意) ユニキャスト ストームしきい値設定を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

interface-id を入力すると、指定されたインターフェイスのストーム制御しきい値が表示されます。

interface-id を入力しない場合、スイッチ上のポートすべてのトラフィック タイプの設定が表示されます。

トラフィック タイプを指定しない場合は、ブロードキャスト ストーム制御の設定が表示されます。

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

次の例では、キーワードを指定せずに入力した **show storm-control** コマンドの出力の一部を示します。トラフィック タイプのキーワードが入力されていないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control
Interface   Filter State  Upper      Lower      Current
-----
Gi0/1      Forwarding   20 pps     10 pps     5 pps
Gi0/2      Forwarding   50.00%    40.00%    0.00%
<output truncated>
```

次の例では、指定のインターフェイスの **show storm-control** コマンドの出力を示します。トラフィック タイプのキーワードが入力されていないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control gigabitethernet 0/1
Interface   Filter State   Upper         Lower         Current
-----
Gi0/1      Forwarding    20 pps       10 pps       5 pps
```

表 2-34 に、**show storm-control** の出力に表示される各フィールドの説明を示します。

表 2-34 show storm-control 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 ID を表示します。
Filter State	フィルタのステータスを表示します。 <ul style="list-style-type: none"> blocking : ストーム制御はイネーブルであり、ストームが発生しています。 forwarding : ストーム制御はイネーブルであり、ストームは発生していません。 Inactive : ストーム制御はディセーブルです。
Upper	上限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Lower	下限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Current	ブロードキャストトラフィックまたは指定のトラフィックタイプ（ブロードキャスト、マルチキャスト、ユニキャスト）の帯域幅の使用状況を、全体で使用可能な帯域幅のパーセンテージで表示します。このフィールドは、ストーム制御がイネーブルの場合のみ有効です。

関連コマンド

コマンド	説明
storm-control	スイッチにブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御レベルを設定します。

表 2-35 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ポート番号
Stack Port Status	<ul style="list-style-type: none"> Absent : ポート上でケーブルが検出されていません。 Down : ケーブルは検出されていますが、接続されたネイバーが動作していないか、または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ており、接続されたネイバーが動作しています。
Neighbor	ケーブルのもう一方の終端のアクティブなメンバーのスイッチ番号

表 2-35 show switch stack-ports summary コマンドの出力 (続き)

フィールド	説明
Cable Length	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、この値は <i>no cable</i> になります。ケーブルが接続されていないか、または信頼できないリンクが使用されている可能性があります。
Link OK	リンクが安定している場合に表示されます。 リンク パートナーとは、ネイバー スイッチ上のポートを意味しています。 <ul style="list-style-type: none"> • No : このポートからリンク パートナーが無効なプロトコル メッセージを受信しました。 • Yes : このポートからリンク パートナーが有効なプロトコル メッセージを受信しました。
Link Active	このポートがリンク パートナーと同じ状態にある場合に表示されます。 <ul style="list-style-type: none"> • No : このポートからリンク パートナーにトラフィックを送信できません。 • Yes : このポートからリンク パートナーにトラフィックを送信できます。
Sync OK	<ul style="list-style-type: none"> • No : リンク パートナーからこの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でした。 • Yes : リンク パートナーからこのポートに有効なプロトコル メッセージが送信されました。
# Changes to LinkOK	リンクの相対的な安定性が表示されます。 短期間のうちに多数の変更が加えられると、リンク フラップが発生する場合があります。
In Loopback	<ul style="list-style-type: none"> • No : メンバー上の少なくとも 1 つのポートにケーブルが接続されています。 • Yes : メンバー上のどのポートにもケーブルが接続されていません。

show system mtu

スイッチに対して設定されたグローバル Maximum Transmission Unit (MTU; 最大伝送ユニット) または最大パケット サイズを表示するには、**show system mtu** 特権 EXEC コマンドを使用します。

show system mtu [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明	
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **system mtu** または **system mtu jumbo** 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 MTU の設定を変更した場合、スイッチをリセットしないかぎり、新しい設定は有効になりません。

システム MTU は 10/100 Mbps で動作するポートを、システム ジャンボ MTU はギガビット ポートを参照します。システム ルーティング MTU はルーテッド ポートを参照します。

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 次の例では、**show system mtu** コマンドの出力を示します。

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1550 bytes
```

■ show system mtu

関連コマンド

コマンド	説明
system mtu	ファストイーサネットポート、ギガビットイーサネットポート、またはル[テッド]ポートの MTU サイズを設定します。

show udld

すべてのポートまたは指定されたポートの UniDirectional Link Detection (UDLD; 単一方向リンク検出) 管理ステータスおよび動作ステータスを表示するには、**show udld** ユーザ EXEC コマンドを使用します。

```
show udld [interface-id] [| {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	(任意) インターフェイスの ID およびポート番号です。指定できるインターフェイスとして、物理ポートおよび VLAN も含まれます。指定できる VLAN 範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

interface-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。

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 がリンクの両端でイネーブルになっており、リンクが双方向であることを UDLD が検出しています。表 2-36 に、この出力で表示される各フィールドの説明を示します。

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
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: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
```

show udld

```
Message interval: 5
CDP Device name: Switch-A
```

表 2-36 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。
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 が近接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	近接デバイスの ID。
Current neighbor state	ネイバーの現在の状態。ローカル デバイスおよび近接装置の両方で 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。
Device name	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装置名。
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。

関連コマンド

コマンド	説明
uddl	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
uddl port	個々のインターフェイスで 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 uddl グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。
uddl reset	UDLD によるすべてのインターフェイス シャットダウンをリセットし、トラフィックが通過するのを再び許可します。

show version

ハードウェアおよびファームウェアのバージョン情報を表示するには、**show version** ユーザ EXEC コマンドを使用します。

show version [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show version** コマンドの出力を示します。



(注)

show version 出力には表示されますが、コンフィギュレーションレジスタ情報はスイッチでサポートされていません。

```
Switch> show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(0.0.16)FX, CISCO
DEVELOPMENT TEST VERSION
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 17-May-05 01:43 by yenh
```

```
ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M), Version 12.2 [lqian-flo_pilsner 100]
```

```
Switch uptime is 3 days, 20 hours, 8 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-0.0.16.FX.bin"
```

```
cisco WS-C2960-24TC-L (PowerPC405) processor with 61440K/4088K bytes of memory.
Processor board ID FHH0916001J
Last reset from power-on
Target IOS Version 12.2(25)FX
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
```

```
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:0B:FC:FF:E8:80
Motherboard assembly number    : 73-9832-02
Motherboard serial number      : FHH0916001J
Motherboard revision number    : 01
System serial number           : FHH0916001J
Hardware Board Revision Number : 0x01
```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
* 1	26	WS-C2960-24TC-L	12.2(0.0.16)FX	C2960-LANBASE-M

```
Configuration register is 0xF
```

show vlan

スイッチ上のすべての設定済の VLAN または特定の 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、**show vlan** ユーザ EXEC コマンドを使用します。

show vlan [**brief** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **remote-span** | **summary**] [| **begin** | **exclude** | **include**] *expression*

シンタックスの説明

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。
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> では、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ユニット (MTU) サイズのリストを表示します。
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。
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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注)

ifindex、**internal usage**、および **private-vlan** キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 を持つポートと MaxMTU を持つポート名が表示されます。

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

次の例では、**show vlan** コマンドの出力を示します。表 2-37 に、この出力で表示されるフィールドの説明を示します。

```
Switch> show vlan
VLAN Name                               Status    Ports
-----
1    default                               active   Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                           Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                           Gi0/9, Gi0/10, Gi0/11, Gi0/12
                                           Gi0/13, Gi0/14, Gi0/15, Gi0/16

<output truncated>

2    VLAN0002                               active
3    VLAN0003                               active

<output truncated>

1000 VLAN1000                             active
1002 fddi-default                         active
1003 token-ring-default                   active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID      MTU   Parent  RingNo  BridgeNo  Stp   BrdgMode  Trans1  Trans2
-----
1    enet    100001   1500  -       -       -       -       -       1002   1003
2    enet    100002   1500  -       -       -       -       -       0      0
3    enet    100003   1500  -       -       -       -       -       0      0

<output truncated>

1005 trnet 101005   1500  -       -       -       -       ibm -       0      0

Remote SPAN VLANs
-----

Primary Secondary Type                Ports
-----
```

表 2-37 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
MTU	VLAN の最大伝送ユニット (MTU) 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)

表 2-37 show vlan コマンドの出力フィールド (続き)

フィールド	説明
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 (STP) タイプ
BrdgMode	この VLAN のブリッジング モード: 可能な値は Source-Route Bridging (SRB; ソースルートブリッジング) および Source-Route Transparent (SRT; ソースルートトランスペアレント) 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。
Primary/Secondary/ Type/Ports	—

次の例では、**show vlan summary** コマンドの出力を示します。

```
Switch> show vlan summary
Number of existing VLANs      : 45
Number of existing VTP VLANs : 45
Number of existing extended VLANs : 0
```

次の例では、**show vlan id** コマンドの出力を示します。

```
Switch# show vlan id 2
VLAN Name                Status    Ports
-----
2    VLAN0200                active    Gi0/1, Gi0/2

2    VLAN0200                active    Fa1/3, Fa2/5, Fa2/6
VLAN Type SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
2    enet  100002  1500  -    -    -    -    -    0    0

Remote SPAN VLAN
-----
Disabled
```

関連コマンド

コマンド	説明
switchport mode	ポートの VLAN メンバシップ モードを設定します。
vlan (グローバル コンフィギュレーション)	VLAN 1 ~ 4094 を設定できる VLAN コンフィギュレーション モードをイネーブルにします。
vlan (VLAN コンフィギュレーション)	VLAN データベースの VLAN 特性を設定します。標準範囲 VLAN (VLAN ID 1 ~ 1005) の場合のみ使用できます。先行ゼロは入力しないでください。

show vmps

VLAN Query Protocol (VQP) バージョン、再確認間隔、再試行回数、VLAN メンバシップ ポリシー サーバ (VMPS) の IP アドレス、および現在のサーバやプライマリ サーバを表示するには、キーワードを指定せずに **show vmps** ユーザ EXEC コマンドを使用します。**statistics** キーワードを指定すると、クライアント側の統計情報が表示されます。

```
show vmps [statistics] [ | {begin | exclude | include} expression]
```

シンタックスの説明

statistics	(任意) VQP のクライアント側統計情報およびカウンタを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show vmps** コマンドの出力を示します。

```
Switch> show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other
```

次の例では、**show vmmps statistics** コマンドの出力を示します。表 2-38 に、表示される各フィールドの説明を示します。

```
Switch> show vmmps statistics
VMPS Client Statistics
-----
VQP Queries:                0
VQP Responses:              0
VMPS Changes:                0
VQP Shutdowns:              0
VQP Denied:                  0
VQP Wrong Domain:           0
VQP Wrong Version:           0
VQP Insufficient Resource:  0
```

表 2-38 show vmmps statistics のフィールドの説明

フィールド	説明
VQP Queries	クライアントから VMPS に送信されるクエリー数。
VQP Responses	VMPS からクライアントに送信される応答数。
VMPS Changes	サーバ間で VMPS を変更した回数。
VQP Shutdowns	ポートをシャットダウンするために VMPS が応答を送信した回数。クライアントはポートをディセーブルにし、このポート上のすべてのダイナミックアドレスをアドレス テーブルから削除します。接続を復元するには、ポートを再び管理上のイネーブル状態にする必要があります。
VQP Denied	VMPS がセキュリティ上の理由からクライアント要求を拒否した回数。VMPS の応答がアドレスを拒否した場合、そのアドレスでワークステーションとのフレーム伝送は実行されません（ポートが VLAN に割り当てられている場合、ブロードキャストまたはマルチキャスト フレームがワークステーションに対して配信されます）。クライアントは拒否されたアドレスをブロック済みアドレスとしてアドレス テーブルに保管します。これにより、このワークステーションから受信した各新規パケットに対するクエリーが、これ以上 VMPS に送信されなくなります。エージング タイム内に、このワークステーションからこのポートに新規パケットが着信しない場合、クライアントはアドレスを期限切れにします。
VQP Wrong Domain	要求内の管理ドメインが VMPS の管理ドメインと一致しない回数。ポートの従来の VLAN 割り当ては変更されません。この応答は、サーバおよびクライアントに同じ VTP 管理ドメインが設定されていないことを意味します。
VQP Wrong Version	クエリー パケットのバージョン フィールドに、VMPS でサポートされているバージョンよりも大きな値が格納されている回数。ポートの VLAN 割り当ては変更されません。スイッチは VMPS バージョン 1 要求のみを送信します。
VQP Insufficient Resource	リソースの可用性に問題があるために、VMPS が要求に応答できない回数。再試行制限に達していない場合、クライアントはサーバごとの再試行回数に達したかどうかに応じて、同じサーバまたは次の代替サーバに要求を再送信します。

関連コマンド

コマンド	説明
clear vmps statistics	VQP クライアントに保持されている統計情報をクリアします。
vmps reconfirm (特権 EXEC)	VQP クエリーを送信して、VMPS でのすべてのダイナミック VLAN 割り当てを再確認します。
vmps retry	VQP クライアントのサーバごとの再試行回数を設定します。
vmps server	プライマリ VMPS および最大で 3 台のセカンダリ サーバを設定します。

show vtp

VLAN トランッキング プロトコル (VTP) の管理ドメイン、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、**show vtp** ユーザ EXEC コマンドを使用します。

```
show vtp {counters | password | status} [| {begin | exclude | include} expression]
```

シンタックスの説明

counters	スイッチの VTP 統計情報を表示します。
password	設定された VTP パスワードを表示します。
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。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

ユーザ EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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

次の例では、**show vtp counters** コマンドの出力を示します。表 2-39 に、表示される各フィールドの説明を示します。

```
Switch> 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 non-pruning-capable device
-----	-----	-----	-----
Fa0/47	0	0	0
Fa0/48	0	0	0
Gi0/1	0	0	0
Gi0/2	0	0	0

表 2-39 show vtp counters の出力に表示される各フィールドの説明

フィールド	説明
Summary advertisements received	トランク ポート上でこのスイッチが受信するサマリー アドバタイズの数。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 ポート上でこのスイッチが受信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つまたは複数の 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 ポート上でこのスイッチが受信するアドバタイズ要求の数。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。
Summary advertisements transmitted	トランク ポート上でこのスイッチが送信するサマリー アドバタイズの数。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 ポート上でこのスイッチが送信するサブセット アドバタイズの数。サブセット アドバタイズには、1 つまたは複数の 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 ポート上でこのスイッチが送信するアドバタイズ要求の数。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、スイッチ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>リビジョン番号がスイッチ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をスイッチが受信すると、リビジョン エラーが増加します。このエラーは、2 つのスイッチの VTP パスワードが異なるか、またはスイッチの設定が異なることを意味します。</p> <p>これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期しなくなります。</p>

表 2-39 show vtp counters の出力に表示される各フィールドの説明 (続き)

フィールド	説明
Number of configuration digest errors	MD5 ダイジェスト エラーの数。 サマリー パケット内の MD5 ダイジェストと、計算された受信済みアドバタイズの 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つのスイッチの 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、すべてのスイッチで VTP パスワードが同じになります。 これらのエラーが発生した場合、スイッチは着信アドバタイズのフィルタリング中であり、ネットワーク内で VTP データベースが同期しなくなります。
Number of V1 summary errors	バージョン 1 エラーの数 VTP V2 モードのスイッチが 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 つの近接スイッチ上で VTP バージョン 1 が稼働しているか、または V2 モードがディセーブルの状態でも VTP バージョン 2 が稼働していることを意味します。この問題を解決するには、VTP V2 モードのスイッチの設定をディセーブルに変更します。
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。

次の例では、**show vtp status** コマンドの出力を示します。表 2-40 に、表示される各フィールドの説明を示します。

```
Switch> show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 45
VTP Operating Mode         : Transparent
VTP Domain Name            : shared_testbed1
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Enabled
MD5 digest                 : 0x3A 0x29 0x86 0x39 0xB4 0x5D 0x58 0xD7
```

表 2-40 show vtp status の各フィールドの説明

フィールド	説明
VTP Version	スイッチ上で稼働している VTP バージョンを表示します。デフォルトでは、スイッチはバージョン 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。
Configuration Revision	このスイッチの現在のコンフィギュレーション リビジョン番号。
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。
VTP Operating Mode	<p>VTP 動作モード（サーバ、クライアント、または透過）を表示します。</p> <p>サーバ：VTP サーバモードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信します。スイッチで VLAN を設定できます。このスイッチを使用すると、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（不揮発性 RAM）から復元できます。デフォルトでは、すべてのスイッチが VTP サーバです。</p> <p>(注) スイッチがコンフィギュレーションを 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ことができない場合、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移行します。</p> <p>クライアント：VTP クライアントモードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信できますが、VLAN コンフィギュレーションを格納するのに十分な不揮発性ストレージが備わっていません。スイッチで VLAN を設定することはできません。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>透過：VTP 透過モードのスイッチは VTP に対してディセーブルであり、アドバタイズの送信も、他のデバイスから送信されたアドバタイズの学習も行いません。また、ネットワーク内の他のデバイス上の VLAN 設定に影響を与えません。スイッチは VTP アドバタイズを受信し、アドバタイズ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>
VTP Domain Name	スイッチ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 V2 Mode	VTP バージョン 2 モードがイネーブルかどうかを表示します。すべての VTP バージョン 2 スイッチは、デフォルトでバージョン 1 モードで動作します。各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP デバイス ネットワーク内のすべての VTP スイッチがバージョン 2 モードで動作可能な場合のみ、ネットワークをバージョン 2 に設定してください。

表 2-40 show vtp status の各フィールドの説明 (続き)

フィールド	説明
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。
MD5 Digest	VTP コンフィギュレーションの 16 バイトチェックサム。
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スイッチの IP アドレスを表示します。

関連コマンド

コマンド	説明
clear vtp counters	VTP およびプルーニング カウンタをクリアします。
vtp (グローバル コンフィギュレーション)	VTP のファイル名、インターフェイス名、ドメイン名、およびモードを設定します。
vtp (VLAN コンフィギュレーション)	VTP のドメイン名、パスワード、プルーニング、およびモードを設定します。

shutdown

インターフェイスをディセーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドを使用します。ディセーブルであるインターフェイスを再起動するには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ポートはイネーブルです（シャットダウンしません）。

コマンド モード インターフェイス コンフィギュレーション

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **shutdown** コマンドを入力すると、ポートは転送を停止します。ポートをイネーブルにするには、**no shutdown** コマンドを使用します。

削除、中断、またはシャットダウンされた VLAN に割り当てられているスタティック アクセス ポートに **no shutdown** コマンドを使用しても、無効です。ポートを再びイネーブルにするには、まずポートをアクティブ VLAN のメンバーにする必要があります。

shutdown コマンドは指定のインターフェイス上のすべての機能をディセーブルにします。

また、インターフェイスが使用不可であることをマーク付けします。インターフェイスがディセーブルかどうかを確認するには、**show interfaces** 特権 EXEC コマンドを使用します。シャットダウンされたインターフェイスは、管理上のダウンとして画面に表示されます。

例 次の例では、ポートをディセーブルにし、次に再びイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown
```

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

コマンド	説明
show interfaces	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に対する統計情報を表示します。

shutdown vlan

指定された VLAN 上のローカルトラフィックをシャットダウン（一時停止）するには、**shutdown vlan** 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。VLAN 上のローカルトラフィックを再開する場合は、このコマンドの **no** 形式を使用します。

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

シンタックスの説明

<i>vlan-id</i>	ローカルにシャットダウンする VLAN の ID です。指定できる範囲は 2 ~ 1001 です。VLAN トランッキング プロトコル (VTP) 環境のデフォルト VLAN として定義された VLAN と ID が 1005 より大きい拡張範囲 VLAN はシャットダウンできません。デフォルト VLAN は 1 および 1002 ~ 1005 です。
----------------	---

デフォルト

デフォルトは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

shutdown vlan コマンドは、VTP データベース内の VLAN 情報を変更しません。このコマンドはローカルトラフィックをシャットダウンしますが、スイッチは VTP 情報をアドバタイズし続けます。

例

次の例では、VLAN 2 のトラフィックをシャットダウンする方法を示します。

```
Switch(config)# shutdown vlan 2
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
shutdown (config-vlan モード)	config-vlan モード (vlan <i>vlan-id</i> グローバル コンフィギュレーション コマンドで開始) の場合に、VLAN のローカルトラフィックをシャットダウンします。
vlan database	VLAN コンフィギュレーション モードを開始します。

small-frame violation rate

指定されたレートで小さいフレーム（67 バイト以下）の VLAN タグ付きパケットを受信した場合にインターフェイスが **errdisable** になるレート（しきい値）を設定するには、**small-frame violation rate pps** 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。

small-frame violation rate pps

no small-frame violation rate pps

シンタックスの説明

pps 小さいフレームを受信したインターフェイスが **errdisable** になるしきい値を指定します。範囲は、1 ~ 10,000 pps です。

デフォルト

この機能は、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、小さいフレームを受信したときにポートが **errdisable** になるレート（しきい値）をイネーブルにします。小さいフレームは、67 以下のフレームと考えられます。

各ポートの小さいフレームのしきい値をグローバルにイネーブルにするには、**errdisable detect cause small-frame** 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。

errdisable recovery cause small-frame 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、ポートが自動的に再びイネーブルになるように設定できます。**errdisable recovery 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、回復時間を設定します。

例

次の例では、小さなフレームが 10,000 pps で着信した場合にポートを **errdisable** にする小さいフレームの着信レート機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# small-frame violation rate 10000
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable detect cause small-frame	着信フレームが最小サイズより小さく、指定されたレート（しきい値）で着信する場合に、スイッチ ポートが errdisable ステートになるようにします。
errdisable recovery cause small-frame	復旧タイマーをイネーブルにします。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。

snmp-server enable traps

スイッチでさまざまなトラップの簡易ネットワーク管理プロトコル (SNMP) 通知を送信したり、ネットワーク管理システム (NMS) に要求を通知したりできるようにするには、**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] | cluster | config |
copy-config | cpu threshold | entity | envmon [fan | shutdown | status | supply |
temperature] | errdisable [notification-rate value] | flash | ipmulticast |
mac-notification | msdp | ospf [cisco-specific | errors | lsa | rate-limit | retransmit |
state-change] | pim [invalid-pim-message | neighbor-change | rp-mapping-change] |
port-security [trap-rate value] | rtr | snmp [authentication | coldstart | linkdown |
linkup | warmstart] | storm-control trap-rate value | stpx [inconsistency]
[root-inconsistency] [loop-inconsistency] | syslog | tty | vlan-membership | vlancreate
| vlandelete | vtp]
```

```
no snmp-server enable traps [bridge [newroot] [topologychange] | cluster | config |
copy-config | cpu threshold | entity | envmon [fan | shutdown | status | supply |
temperature] | errdisable [notification-rate] | flash | ipmulticast | mac-notification |
msdp | ospf [cisco-specific | errors | lsa | rate-limit | retransmit | state-change] | pim
[invalid-pim-message | neighbor-change | rp-mapping-change] | port-security
[trap-rate] | rtr | snmp [authentication | coldstart | linkdown | linkup | warmstart] |
storm-control trap-rate | stpx [inconsistency] [root-inconsistency]
[loop-inconsistency] | syslog | tty | vlan-membership | vlancreate | vlandelete | vtp]
```

シンタックスの説明

bridge [newroot] [topologychange]	(任意) スパニングツリー プロトコル (STP) ブリッジ MIB (管理情報ベース) トラップを生成します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> newroot : (任意) SNMP STP ブリッジ MIB の新しいルート トラップをイネーブルにします。 topologychange : (任意) SNMP STP ブリッジ MIB のトポロジ変更トラップをイネーブルにします。
cluster	(任意) クラスタ 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。
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 threshold	(任意) CPU に関連したトラップをイネーブルにします。 このキーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。
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 [fan shutdown status supply temperature]	(任意) SNMP 環境トラップをイネーブルにします。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • fan : (任意) ファン トラップをイネーブルにします。 • shutdown : (任意) 環境モニタ シャットダウン トラップをイネーブルにします。 • 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。 • supply : (任意) 環境モニタ電源トラップをイネーブルにします。 • temperature : (任意) 環境モニタ温度トラップをイネーブルにします。
errdisable [notification-rate value]	(任意) errdisable トラップをイネーブルにします。notification-rate キーワードを使用して、毎分送信される errdisable トラップの最大値を設定します。指定できる範囲は 0 ~ 10000 です。デフォルト値は 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)。
flash	(任意) SNMP FLASH 通知をイネーブルにします。
ipmulticast	(任意) IP マルチキャスト ルーティング トラップをイネーブルにします。
mac-notification	(任意) MAC (メディア アクセス制御) アドレス通知トラップをイネーブルにします。
msdp	(任意) Multicast Source Discovery Protocol (MSDP) トラップをイネーブルにします。
ospf [cisco-specific errors lsa rate-limit retransmit state-change]	(任意) Open Shortest Path First (OSPF) トラップをイネーブルにします。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • 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) Link-State Advertisement (LSA; リンクステートアドバタイズメント) トラップをイネーブルにします。 • rate-limit : (任意) 速度制限トラップをイネーブルにします。 • 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) ステータス変更トラップをイネーブルにします。
pim [invalid-pim-message neighbor-change rp-mapping-change]	(任意) Protocol-Independent Multicast (PIM) トラップをイネーブルにします。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • 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) Rendezvous Point (RP) マッピング変更トラップをイネーブルにします。
port-security [trap-rate value]	(任意) ポートセキュリティ トラップをイネーブルにします。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するには、 trap-rate キーワードを使用します。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 (制限はなく、トラップをすべての発生原因にたいして送信) です。
rtr	(任意) SNMP Response Time Reporter トラップをイネーブルにします。 このキーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。

snmp [authentication coldstart linkdown linkup warmstart]	(任意) SNMP トラップをイネーブルにします。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • 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。
storm-control trap-rate value	(任意) ストーム制御トラップをイネーブルにします。分単位で送信されるストーム制御トラップの最大数を設定するには、 trap-rate キーワードを使用します。指定できる範囲は 0 ~ 1000 です。デフォルト値は 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)。
stpx	(任意) SNMP STPX MIB トラップをイネーブルにします。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • inconsistency : (任意) SNMP STPX MIB の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 のルート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 のループ矛盾更新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。
tty	(任意) TCP 接続トラップを送信します。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。
vtp	(任意) VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) トラップをイネーブルにします。



(注)

hsrp、**insertion**、**removal**、および **rtr** キーワードは、コマンドラインのヘルプ スtring に表示されますが、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て使用します。

デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(37)SE	errdisable notification-rate value キーワードが追加されました。
12.2(50)SE	cpu threshold キーワードが追加されました。

使用上のガイドライン

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。

snmp-server enable traps コマンドは、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します。



(注)

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。

CPU しきい値通知のタイプと値を設定するには、**process cpu threshold type** 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。

例

次の例では、NMS に VTP トラップを送信する方法を示します。

```
Switch(config)# snmp-server enable traps vtp
```

設定を確認するには、**show vtp status** 特権 EXEC コマンド、または **show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。
snmp-server host	SNMP トラップを受信するホストを指定します。

snmp-server host

SNMP 通知処理の受信側（ホスト）を指定するには、**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。指定され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 [informs | traps] [version {1 | 2c | 3 {auth | noauth | priv}}] [vrf vrf-instance] {community-string [notification-type]}
```

```
no snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 {auth | noauth | priv}}] [vrf vrf-instance] community-string
```

シンタックスの説明

<i>host-addr</i>	ホストの名前またはインターネット アドレス（ターゲットとなる受信側）です。
udp-port <i>port</i>	（任意）トラップを受信するホストの User Datagram Protocol (UDP) ポート番号を設定します。指定できる範囲は 0 ~ 65535 です。
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 のバージョンです。 次のキーワードがサポートされています。 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。バージョン 3 キーワードのあとに、次に示すオプションキーワードを指定できます。 <ul style="list-style-type: none"> auth（任意）：MD5 および Secure Hash Algorithm (SHA) によるパケット認証をイネーブルにします。 noauth（デフォルト）：noAuthNoPriv というセキュリティ レベルです。[auth noauth priv] キーワードが指定されていない場合は、これがデフォルトです。 priv（任意）：Data Encryption Standard (DES; データ暗号化規格) 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。 (注) priv キーワードは、暗号化ソフトウェア イメージがインストールされている場合にだけ利用できます。
vrf <i>vrf-instance</i>	（任意）Virtual Private Network (VPN; バーチャル プライベート ネットワーク) ルーティング インスタンスとホスト名です。

community-string

通知処理によ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、次に **snmp-server host** コマンドを使用することを推奨します。

(注) @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定する場合は、SNMP コミュニティ ストリングとして @ 記号を使用しないようにしてください。

notification-type

(任意) ホストに送信される通知のタイプ。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。

- **bridge** : (任意) 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。
 - **cluster** : クラスタ メンバー ステータス トラップを送信します。
 - **config** : SNMP 設定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 threshold** : CPU に関連したトラップを許可します。このキーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。
 - **entity** : SNMP エンティティ 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 通知を送信します。
 - **flash** : SNMP FLASH 通知を送信します。
 - **hsrp** : SNMP Hot Standby Router Protocol (HSRP) 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。
 - **mac-notification** : SNMP MAC (メディア アクセス制御) 通知トラップを送信します。
 - **msdp** : SNMP Multicast Source Discovery Protocol (MSDP) トラップを送信します。
 - **ospf** : Open Shortest Path First (OSPF) トラップを送信します。
 - **pim** : SNMP Protocol-Independent Multicast (PIM) トラップを送信します。
 - **port-security** : SNMP ポートセキュリティ トラップを送信します。
 - **rtr** : SNMP Response Time Reporter 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。
 - **stpx** : 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。
 - **tty** : TCP 接続トラップを送信します。
 - **udp-port port** : トラップを受信するホストの User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ポート番号を設定します。指定できる範囲は 0 ~ 65535 です。
 - **vlan-membership** : SNMP VLAN メンバシップ トラップを送信します。
 - **vlancreate** : SNMP VLAN 作成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。
 - **vtp** : SNMP VLAN トランッキング プロトコル (VTP) トラップを送信します。
-

デフォルト

このコマンドは、デフォルトではディセーブルです。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。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(37)SE	errdisable notification-rate value キーワードが追加されました。
12.2(50)SE	cpu threshold キーワードが追加されました。

使用上のガイドライン

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かった場合は、再び情報要求を送信できます。したがって、情報が目的の宛先に到達する可能性が高まります。

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。送信と同時にドロップされるトラップと異なり、情報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。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなります。

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スイッチを設定するには、少なくとも 1 つの **snmp-server host** コマンドを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は、ホストに対して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。ホストごとのコマンドでは、複数の通知タイプを指定できます。

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、スイッチは **auth** (authNoPriv) および **priv** (authPriv) 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に対して複数の **snmp-server host** コマンドを指定した場合は、あとの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** コマンドのみが有効です。たとえば、ホストに **snmp-server host inform** 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せん。

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 つのホストが大部分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** コマンドおよび **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化されます。

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。

例

次の例では、トラップに対して一意の SNMP コミュニティ ストリング *comaccess* を設定し、このストリングによる、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。

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(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 ストリングは、*comaccess* として定義されています。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする方法を示します。

```
Switch(config)# snmp-server enable traps
Switch(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。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
snmp-server enable traps	各トラップ タイプまたは情報要求の SNMP 通知をイネーブルにします。

snmp trap mac-notification

特定のレイヤ 2 インターフェイス上で SNMP MAC アドレス通知トラップをイネーブルにするには、**snmp trap mac-notification** 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。

snmp trap mac-notification {added | removed}

no snmp trap mac-notification {added | removed}

シンタックスの説明

added	MAC アドレスがインターフェイスに追加されるたびに、MAC 通知トラップをイネーブルにします。
removed	MAC アドレスがインターフェイスから削除されるたびに、MAC 通知トラップをイネーブルにします。

デフォルト

デフォルトでは、アドレス追加および削除に対するトラップは両方ディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

snmp trap mac-notification コマンドを使用して、特定のインターフェイスの通知トラップをイネーブルにできますが、トラップが生成されるのは、**snmp-server enable traps mac-notification** および **mac address-table notification** グローバル コンフィギュレーション コマンドをイネーブルにした場合のみです。

例

次の例では、MAC アドレスがポートに追加されたときに MAC 通知トラップをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification added
```

設定を確認するには、**show mac address-table notification interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
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-server enable traps	mac-notification キーワードが追加された場合に SNMP MAC 通知トラップを送信します。

spanning-tree backbonefast

BackboneFast 機能をイネーブルにするには、**spanning-tree backbonefast** 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。

spanning-tree backbonefast

no spanning-tree backbonefast

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

BackboneFast はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

BackboneFast 機能は、Rapid PVST+ または Multiple Spanning-Tree (MST) モード用に設定できますが、Spanning Tree モードを PVST+ に変更するまでこの機能はディセーブル (非アクティブ) のままです。

スイッチのルート ポートまたはブロックされたポートが、指定されたスイッチから不良ブリッジプロトコル データ ユニット (BPDU) を受信すると、BackboneFast が開始されます。下位 BPDU は、ルートブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク (間接リンク) で障害が発生したことを意味します (指定スイッチとルートスイッチ間の接続が切断されています)。ルートスイッチへの代替パスがある場合に BackboneFast を使用すると、不良 BPDU を受信するインターフェイスの最大エージング タイムが期限切れになり、ブロックされたポートをただちにリスニング ステートに移行できます。そのあと、BackboneFast はインターフェイスをフォワーディング ステートに移行させます。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。

間接リンク障害を検出できるようにしたり、Spanning Tree の再認識をより短時間で開始したりするには、サポートされるすべてのスイッチで BackboneFast をイネーブルにしてください。

例

次の例では、スイッチ上で BackboneFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree backbonefast
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>show spanning-tree summary</code>	スパニングツリー インターフェイス ステートのサマリーを表示します。

spanning-tree bpdudfilter

インターフェイス上での BPDU の送受信を禁止するには、**spanning-tree bpdudfilter** 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。

spanning-tree bpdudfilter {disable | enable}

no spanning-tree bpdudfilter

シンタックスの説明

disable	指定されたインターフェイス上で BPDU フィルタリングをディセーブルにします。
enable	指定された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。

デフォルト

BPDU フィルタリングはディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ モード、または Multiple Spanning-Tree (MST) モードで稼動している場合は、BPDU フィルタリング機能をイネーブルにできません。



注意

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

すべての PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast bpdudfilter default** 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。

spanning-tree portfast bpdudfilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdudfilter** 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。

例

次の例では、ポート上で BPDU フィルタリング機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdudfilter enable
```

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。

関連コマンド	コマンド	説明
	show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
	spanning-tree portfast (グローバル コンフィギュレーション)	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
	spanning-tree portfast (インターフェイス コンフィギュレーション)	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree bpduguard

BPDU を受信したインターフェイスを errdisable ステートにするには、**spanning-tree bpduguard** 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。

spanning-tree bpduguard {disable | enable}

no spanning-tree bpduguard

シンタックスの説明

disable	指定されたインターフェイス上で BPDU ガードをディセーブルにします。
enable	指定されたインターフェイス上で BPDU ガードをイネーブルにします。

デフォルト

BPDU ガードはディセーブルです。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスを手動で再び動作する必要がある場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でインターフェイスがスパンニングツリー トポロジに追加されないようにするには、BPDU ガード機能を使用します。

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ モード、または Multiple Spanning-Tree (MST) モードで稼働している場合は、BPDU ガード機能をイネーブルにできます。

すべての PortFast 対応インターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast bpduguard default** 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。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpduguard** 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。

例

次の例では、ポートで BPDU ガード機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

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。

関連コマンド	コマンド	説明
	show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
	spanning-tree portfast (グローバル コンフィギュレーション)	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
	spanning-tree portfast (インターフェイス コンフィギュレーション)	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree cost

スパニングツリーの計算に使用するパス コストを設定するには、**spanning-tree cost** 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。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。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*] cost *cost*

no spanning-tree [vlan *vlan-id*] cost

シンタックスの説明

vlan <i>vlan-id</i>	(任意) スパニングツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
<i>cost</i>	パス コスト。使用できる範囲は 1 ~ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mb/s : 4
- 100 Mb/s : 19
- 10 Mb/s : 100

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

spanning-tree vlan *vlan-id* cost *cost* コマンドおよび **spanning-tree cost *cost*** コマンドの両方を使用してインターフェイスを設定する場合、**spanning-tree vlan *vlan-id* cost *cost*** コマンドが有効になります。

例

次の例では、ポートでパス コストを 250 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

次の例では、VLAN 10、12 ~ 15、および 20 に対してパス コスト 300 を設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

設定を確認するには、**show spanning-tree interface *interface-id*** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface <i>interface-id</i>	特定のインターフェイスのスパニングツリー情報を表示します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree etherchannel guard misconfig

スイッチが EtherChannel の設定ミスを検出した場合にエラーメッセージを表示するには、**spanning-tree etherchannel guard misconfig** 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。機能をディisableにする場合は、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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

EtherChannel ガードはスイッチでイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが EtherChannel の設定ミスを検出すると、次のエラー メッセージが表示されます。

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in err-disable state.
```

設定ミスの EtherChannel にあるスイッチ ポートを表示するには、**show interfaces status err-disabled** 特権 EXEC コマンドを使用します。リモート デバイスの EtherChannel 設定を確認するには、リモート デバイスで **show etherchannel summary** 特権 EXEC コマンドを使用します。

EtherChannel の設定矛盾によりポートが **errdisable** ステートの場合は、**errdisable recovery cause channel-misconfig** 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したり、**shutdown** および **no shut down** 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、手動で再度イネーブルにすることができます。

例

次の例では、EtherChannel ガードの設定ミス機能をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable recovery cause channel-misconfig	EtherChannel の設定矛盾による 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。
show etherchannel summary	チャンネルの EtherChannel 情報を、チャンネルグループ単位で 1 行のサマリーとして表示します。
show interfaces status err-disabled	errdisable ステートのインターフェイスを表示します。

spanning-tree extend system-id

拡張システム ID 機能をイネーブルにするには、**spanning-tree extend system-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。

spanning-tree extend system-id



(注)

このコマンドの **no** バージョンは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。拡張システム ID 機能をディセーブルにすることはできません。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

拡張システム ID はイネーブルです。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチは、IEEE 802.1t スパニングツリー拡張をサポートします。以前スイッチ プライオリティに使用されたビットの一部は現在、拡張システム ID (Per-VLAN Spanning-Tree Plus [PVST+] と Rapid PVST+ の VLAN 識別子、または Multiple Spanning-Tree [MST] のインスタンス識別子) に使用しません。

スパニングツリーは、ブリッジ ID が VLAN または MST インスタンスごとに一意となるようにするために、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用しています。

拡張システム ID のサポートにより、ルートスイッチ、セカンダリ ルートスイッチ、および VLAN のスイッチ プライオリティを手動で設定する方法に影響が生じます。詳細については、「[spanning-tree mst root](#)」および「[spanning-tree vlan](#)」を参照してください。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルートスイッチになることはほぼありません。拡張システム ID によって、接続されたスイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

関連コマンド

コマンド	説明
<code>show spanning-tree summary</code>	スパニングツリー インターフェイス ステートのサマリーを表示します。
<code>spanning-tree mst root</code>	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
<code>spanning-tree vlan priority</code>	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree guard

選択したインターフェイスに関連付けられたすべての VLAN 上でルートガードまたはループガードをイネーブルにするには、**spanning-tree guard** 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。ルートガードは、スパニングツリー ルートポートまたはスイッチのルートへのパスになることが可能なインターフェイスを制限します。ループガードは、障害によって単一方向リンクが作成された場合に、代替ポートまたはルートポートが指定ポートにならないようにします。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 | none | root}

no spanning-tree guard

シンタックスの説明

loop	ループガードをイネーブルにします。
none	ルートガードまたはループガードをディセーブルにします。
root	ルートガードをイネーブルにします。

デフォルト

ルートガードはディセーブルです。

ループガードは、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドに従って設定されます（グローバルにディセーブル化）。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ モード、または Multiple Spanning-Tree (MST) モードで稼動している場合は、ルートガードまたはループガード機能をイネーブルにできます。

ルートガードがイネーブルの場合に、スパニングツリーを計算すると、インターフェイスがルートポートとして選択され、**root-inconsistent** (ブロック) ステートに移行します。これにより、カスタマーのスイッチがルートスイッチになったり、ルートへのパスになったりすることがなくなります。ルートポートは、スイッチからルートスイッチまでの最適パスを提供します。

no spanning-tree guard または **no spanning-tree guard none** コマンドを入力すると、ルートガードは選択されたインターフェイスのすべての VLAN でディセーブルになります。このインターフェイスが **root-inconsistent** (ブロック) ステートの場合、インターフェイスはリスニングステートに自動的に移行します。

UplinkFast 機能が使用するインターフェイスで、ルートガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に (ブロッキングステートの) バックアップインターフェイスがルートポートになります。しかし、同時にルートガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップインターフェイスが **root-inconsistent** (ブロック) になり、フォワーディングステートに移行できなくなります。スイッチが Rapid PVST+ モードまたは MST モードで稼動している場合は、UplinkFast 機能は使用できません。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid PVST+ モードで稼動している場合は、ループ ガードによって代替ポートとルート ポートが指定のポートにならなくなり、スパニングツリーによって代替ポート上でもルート ポート上でも BPDU が送信されなくなります。スイッチが MST モードで稼動している場合は、すべての MST インスタンスでこのインターフェイスがループ ガードによってブロックされている場合のみ、非境界インターフェイスから BPDU が送信されなくなります。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ルート ガードまたはループ ガードをディセーブルにする場合は、**spanning-tree guard none** 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。ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** 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。

例

次の例では、指定のポートに関連付けられたすべての VLAN で、ルート ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

次の例では、指定のポートに関連付けられたすべての VLAN 上でループ ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

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。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree loopguard default	単一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ないようにします。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree link-type

インターフェイスのデュプレックス モードによって決まるデフォルトのリンクタイプ設定を無効化し、フォワーディング ステートへの高速スパンニングツリーの移行をイネーブルにするには、**spanning-tree link-type** 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。

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

シンタックスの説明

point-to-point	インターフェイスのリンク タイプがポイントツーポイントであることを指定します。
shared	インターフェイスのリンク タイプが共有であることを指定します。

デフォルト

スイッチは、デュプレックス モードからインターフェイスのリンク タイプを取得します。つまり、全二重インターフェイスはポイントツーポイント リンクであると見なされ、半二重インターフェイスは共有リンクであると見なされます。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

リンク タイプのデフォルト設定を上書きするには、**spanning-tree link-type** コマンドを使用します。たとえば、半二重リンクは、Multiple Spanning-Tree Protocol (MSTP) または Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+) プロトコルが稼動し高速移行がイネーブルであるリモート スイッチの 1 つのインターフェイスに、ポイントツーポイントで物理的に接続できます。

例

次の例では、(デュプレックスの設定に関係なく) リンク タイプを共有に指定し、フォワーディング ステートへの高速移行を禁止する方法を示します。

```
Switch(config-if)# spanning-tree link-type shared
```

設定を確認するには、**show spanning-tree mst interface interface-id** または **show spanning-tree interface interface-id** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear spanning-tree detected-protocols	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でプロトコル移行プロセスを再開（強制的に近接スイッチと再びネゴシエートさせる）します。
show spanning-tree interface interface-id	特定のインターフェイスのスパニングツリー ステート情報を表示します。
show spanning-tree mst interface interface-id	特定のインターフェイスの MST 情報を表示します。

spanning-tree loopguard default

単一方向リンクを発生させる障害が原因で代替ポートまたはルートポートが指定のポートになることを防ぐには、**spanning-tree loopguard default** 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。

spanning-tree loopguard default

no spanning-tree loopguard default

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ループ ガードはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ モード、または Multiple Spanning-Tree (MST) モードで稼動している場合は、ループ ガード機能をイネーブルにできます。

ループ ガード機能は、スイッチド ネットワーク 全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid PVST+ モードで稼動している場合、ループ ガードによって、代替ポートおよびルートポートは指定ポートになることがなく、スパンニング ツリーはルートポートまたは代替ポートでブリッジ プロトコル データ ユニット (BPDU) を送信しません。スイッチが MST モードで稼動している場合は、すべての MST インスタンスでこのインターフェイスがループ ガードによってブロックされている場合のみ、非境界インターフェイスから BPDU が送信されなくなります。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ループ ガードは、スパンニング ツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** 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。

例

次の例では、ループ ガードをグローバルにイネーブルにします。

```
Switch(config)# spanning-tree loopguard default
```

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。

関連コマンド

コマンド	説明
<code>show running-config</code>	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
<code>spanning-tree guard loop</code>	指定したインターフェイスに関連付けられたすべての VLAN で、ループガード機能をイネーブルにします。

spanning-tree mode

スイッチ上で Per-VLAN Spanning-Tree Plus (PVST+)、Rapid-PVST+、または Multiple Spanning-Tree (MST) をイネーブルにするには、**spanning-tree mode** + 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。

spanning-tree mode {mst | pvst | rapid-pvst}

no spanning-tree mode

シンタックスの説明

mst	MST および Rapid Spanning-Tree Protocol (RSTP) をイネーブルにします (IEEE 802.1s および IEEE 802.1w に準拠)。
pvst	PVST+ をイネーブルにします (IEEE 802.1D に準拠)。
rapid-pvst	Rapid-PVST+ をイネーブルにします (IEEE 802.1w に準拠)。

デフォルト

デフォルト モードは PVST+ です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチは PVST+、Rapid PVST+、および MSTP をサポートしていますが、常時アクティブにできるのは 1 つのバージョンだけです。すべての VLAN で PVST+ が実行されるか、すべての VLAN で Rapid-PVST+ が実行されるか、またはすべての VLAN で MSTP が実行されます。

MST モードをイネーブルにした場合、RSTP が自動的にイネーブルになります。



注意

スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが以前のモードのために停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。

例

次の例では、スイッチ上で MST および RSTP をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode mst
```

次の例では、スイッチ上で Rapid-PVST+ をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode rapid-pvst
```

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。

関連コマンド

コマンド	説明
<code>show running-config</code>	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」 > 「File Management Commands」 > 「Configuration File Management Commands」を選択してください。

spanning-tree mst configuration

Multiple Spanning-Tree (MST) リージョンを設定する場合に使用する MST コンフィギュレーションモードを開始するには、**spanning-tree mst configuration** 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。

spanning-tree mst configuration

no spanning-tree mst configuration

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、すべての VLAN（仮想 LAN）が Common and Internal Spanning-Tree (CIST) インスタンス（インスタンス 0）にマッピングされます。

デフォルト名は空の文字列です。

リビジョン番号は 0 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	<i>instance-id</i> の範囲が 1 ~ 4094 に変更されました。

使用上のガイドライン

MST コンフィギュレーション モードをイネーブルにするには、**spanning-tree mst configuration** コマンドを使用します。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。

- **abort** : 設定変更を適用せずに MST リージョン コンフィギュレーション モードを終了します。
- **exit** : MST リージョン コンフィギュレーション モードを終了し、すべての設定変更を適用します。
- **instance *instance-id* vlan *vlan-range*** : VLAN を MST インスタンスにマッピングします。指定できる *instance-id* の範囲は 1 ~ 4094 です。指定できる *vlan-range* の範囲は 1 ~ 4094 です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。
- **name *name*** : 設定名を指定します。 *name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。
- **no : instance、name、および revision** コマンドを無視するか、またはデフォルト設定に戻します。
- **private-vlan** : このコマンドは、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。
- **revision *version*** : 設定のリビジョン番号を指定します。指定できる範囲は 0 ~ 65535 です。
- **show [current | pending]** : 現在の MST リージョン設定または保留中の MST リージョン設定を表示します。

MST モードでは、スイッチは最大 65 の MST インスタンスまでサポートします。特定の MST インスタンスにマッピング可能な VLAN 数は制限されていません。

VLAN を MST インスタンスにマッピングすると、マッピングは差分で実行され、コマンドで指定された VLAN が以前マッピングされた VLAN に追加または VLAN から削除されます。範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** と指定すると、MST インスタンス 1 に VLAN 1 ~ 63 がマッピングされます。列挙を指定する場合は、カンマを使用します。たとえば、**instance 1 vlan 10, 20, 30** と指定すると、MST インスタンス 1 に VLAN 10、20、および 30 がマッピングされます。

明示的に MST インスタンスにマッピングされていないすべての VLAN は、CIST インスタンス（インスタンス 0）にマッピングされます。このマッピングは、このコマンドの **no** 形式では解除できません。

2 台以上のスイッチが同一 MST リージョン内に存在するには、同じ VLAN マッピング、同じ構成リビジョン番号、および同じ名前が設定されている必要があります。

例

次の例では、MST コンフィギュレーション モードを開始して VLAN 10 ~ 20 を MST インスタンス 1 にマッピングし、リージョンに *region1* と名前を付けて、構成リビジョンを 1 に設定します。変更確認前の構成を表示して変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----  -
0          1-9,21-4094
1          10-20
-----

Switch(config-mst)# exit
Switch(config)#
```

次の例では、インスタンス 2 にすでにマッピングされている VLAN があれば、そこに VLAN 1 ~ 100 を追加し、インスタンス 2 にマッピングされていた VLAN 40 ~ 60 を CIST インスタンスに移動し、インスタンス 10 に VLAN 10 を追加し、インスタンス 2 にマッピングされたすべての VLAN を削除し、それらを CIST インスタンスにマッピングする方法を示します。

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

設定を確認するには、**show pending MST** コンフィギュレーション コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst configuration	MST リージョンの設定を表示します。

spanning-tree mst cost

Multiple Spanning-Tree (MST) の計算に使用するパス コストを設定するには、**spanning-tree mst cost** 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。ループが発生した場合、スパンニング 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。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 cost cost

no spanning-tree mst instance-id cost

シンタックスの説明	
<i>instance-id</i>	スパンニングツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ~ 4094 です。
<i>cost</i>	パス コストの範囲は 1 ~ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mb/s : 20000
- 100 Mb/s : 200000
- 10 Mb/s : 2000000

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	<i>instance-id</i> の範囲が 1 ~ 4094 に変更されました。

使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

例

次の例では、インスタンス 2 および 4 に関連付けられたポートにパス コストとして 250 を設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

設定を確認するには、**show spanning-tree mst interface interface-id** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>show spanning-tree mst interface <i>interface-id</i></code>	特定のインターフェイスの MST 情報を表示します。
<code>spanning-tree mst port-priority</code>	インターフェイス プライオリティを設定します。
<code>spanning-tree mst priority</code>	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst forward-time

すべての Multiple Spanning-Tree (MST) インスタンスの転送遅延時間を設定するには、**spanning-tree mst forward-time** 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。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を指定します。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

シンタックスの説明	<i>seconds</i>	リスニングおよびラーニング ステートの期間です。指定できる範囲は 4 ~ 30 秒です。
------------------	----------------	--

デフォルト デフォルト値は 15 秒です。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **spanning-tree mst forward-time** コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例 次の例では、すべての MST インスタンスについて、スパニングツリーの転送時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst forward-time 18
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show spanning-tree mst	MST 情報を表示します。
	spanning-tree mst hello-time	ルートスイッチ コンフィギュレーションメッセージから送信される hello BPDU (ブリッジ プロトコル データ ユニット) の間隔を設定します。
	spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。
	spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst hello-time

ルートスイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔を設定するには、**spanning-tree mst hello-time** 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。

spanning-tree mst hello-time seconds

no spanning-tree mst hello-time

シンタックスの説明	<i>seconds</i>	ルートスイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔です。指定できる範囲は 1 ~ 10 秒です。
------------------	----------------	---

デフォルト デフォルト値は 2 秒です。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **spanning-tree mst max-age seconds** グローバル コンフィギュレーション コマンドを設定したあとに、指定された期間内にルート スイッチから BPDU を受信しない場合、スイッチはスパニングツリー トポロジを再計算します。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst hello-time コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例 次の例では、すべての MST インスタンスについて、スパニングツリーの hello タイムを 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst hello-time 3
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	show spanning-tree mst	MST 情報を表示します。
	spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
	spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。
	spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst max-age

スパニングツリーがルート スイッチからメッセージを受信する間隔を設定するには、**spanning-tree mst max-age** 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。スイッチがこのインターバル内にルート スイッチからブリッジプロトコル データ ユニット (BPDU) メッセージを受信しない場合は、スパニングツリー トポロジが再計算されます。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

シンタックスの説明

<i>seconds</i>	スパニング ツリーがルート スイッチからメッセージを受信する間隔です。指定できる範囲は 6 ~ 40 秒です。
----------------	---

デフォルト

デフォルト値は 20 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst max-age seconds グローバル コンフィギュレーション コマンドを設定したあとに、指定された期間内にルート スイッチから BPDU を受信しない場合、スイッチはスパニングツリー トポロジを再計算します。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst max-age コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree (MST) インスタンスについて、スパニングツリーの有効期間を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-age 30
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。

コマンド	説明
<code>spanning-tree mst hello-time</code>	ルートスイッチコンフィギュレーションメッセージが送信する hello BPDU の間隔を設定します。
<code>spanning-tree mst max-hops</code>	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst max-hops

BPDU が廃棄されて、インターフェイスに保持された情報が期限切れになるまでのリージョンのホップ数を設定するには、**spanning-tree mst max-hops** 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。

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

シンタックスの説明

hop-count BPDU が廃棄されるまでのリージョンのホップ数です。指定できるホップ数は 1 ～ 255 です。

デフォルト

デフォルトのホップ数は 20 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	<i>hop-count</i> の範囲は 1 ～ 255 に変更されました。

使用上のガイドライン

インスタンスのルート スイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。スイッチは、BPDU を受信すると、受信した残りのホップ カウントを 1 つ減らして、生成する M レコードの残りのホップ カウントとしてこの値を伝播します。ホップ カウントが 0 になると、スイッチは BPDU を廃棄して、インターフェイスに保持された情報を期限切れにします。

spanning-tree mst max-hops コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree (MST) インスタンスについて、スパニングツリーの最大ホップ数を 10 に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-hops 10
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>show spanning-tree mst</code>	MST 情報を表示します。
<code>spanning-tree mst forward-time</code>	すべての MST インスタンスについて転送遅延時間を設定します。
<code>spanning-tree mst hello-time</code>	ルートスイッチコンフィギュレーションメッセージが送信する hello BPDU の間隔を設定します。
<code>spanning-tree mst max-age</code>	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。

spanning-tree mst port-priority

インターフェイス プライオリティを設定するには、**spanning-tree mst port-priority** 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。ループが発生した場合、Multiple Spanning-Tree Protocol (MSTP) はフォワーディング ステートに設定するインターフェイスを判別できます。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。

spanning-tree mst *instance-id* port-priority *priority*

no spanning-tree mst *instance-id* port-priority

シンタックスの説明	
<i>instance-id</i>	スパニングツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ~ 4094 です。
<i>priority</i>	指定できる範囲は 0 ~ 240 であり、刻み幅は 16 です。有効なプライオリティ値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	<i>instance-id</i> の範囲が 1 ~ 4094 に変更されました。

使用上のガイドライン

最初に選択させるインターフェイスには高いプライオリティ（小さい数値）を与え、最後に選択させるインターフェイスには低いプライオリティ（大きい数値）を付けます。すべてのインターフェイスに同じプライオリティ値が付けられている場合、Multiple Spanning-Tree (MST) はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

例

次の例では、ループが発生した場合に、スパニングツリー インスタンス 20 および 22 に関連付けられたインターフェイスがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

設定を確認するには、**show spanning-tree mst interface *interface-id*** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
<code>show spanning-tree mst interface interface-id</code>	特定のインターフェイスの MST 情報を表示します。
<code>spanning-tree mst cost</code>	MST の計算に使用するパス コストを設定します。
<code>spanning-tree mst priority</code>	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst pre-standard

ポートが先行標準ブリッジプロトコルデータユニット (BPDU) のみを送信するように設定するには、**spanning-tree mst pre-standard** 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。

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

デフォルトのステートは、先行標準ネイバーの自動検出です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

ポートでは、先行標準と標準の両方の BPDU を受け入れることができます。ネイバー タイプが不一致の場合、Common and Internal Spanning-Tree (CIST) のみがこのインターフェイスで実行されます。



(注)

スイッチのポートが、先行標準の Cisco IOS ソフトウェアを実行しているスイッチに接続されている場合には、ポートに対して **spanning-tree mst pre-standard** 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必要があります。ポートが先行標準 BPDU のみを送信するように設定していない場合、Multiple STP (MSTP) のパフォーマンスが低下することがあります。

自動的に先行標準ネイバーを検出するようにポートが設定されている場合、**show spanning-tree mst** コマンドに *prestandard* フラグが常に表示されます。

例

次の例では、ポートが先行標準 BPDU のみを送信するように設定する方法を示します。

```
Switch(config-if)# spanning-tree mst pre-standard
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst instance-id	<i>prestandard</i> フラグなど、指定されたインターフェイスの Multiple Spanning-Tree (MST) 情報を表示します。

spanning-tree mst priority

指定されたスパンニングツリー インスタンスに対してスイッチのプライオリティを設定するには、**spanning-tree mst priority** 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。

spanning-tree mst *instance-id* priority *priority*

no spanning-tree mst *instance-id* priority

シンタックスの説明

<i>instance-id</i>	スパンニングツリー インスタンス範囲。1つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ~ 4094 です。
<i>priority</i>	指定したスパンニングツリー インスタンスのスイッチ プライオリティを設定します。この設定は、スイッチがルート スイッチとして選択される可能性に影響します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ~ 61440 であり、刻み幅は 4096 です。有効なプライオリティ値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。それ以外の値はすべて拒否されます。

デフォルト

デフォルト値は 32768 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	<i>instance-id</i> の範囲が 1 ~ 4094 に変更されました。

例

次の例では、Multiple Spanning-Tree (MST) インスタンス 20 ~ 21 のスパンニングツリー プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

設定を確認するには、**show spanning-tree mst *instance-id*** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst <i>instance-id</i>	特定のインターフェイスの MST 情報を表示します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。

spanning-tree mst root

ネットワークの直径に基づいて Multiple Spanning-Tree (MST) ルートスイッチのプライオリティとタイマーを設定するには、**spanning-tree mst root** 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。

```
spanning-tree mst instance-id root {primary | secondary} [diameter net-diameter
[hello-time seconds]]
```

```
no spanning-tree mst instance-id root
```

シンタックスの説明

<i>instance-id</i>	スパニングツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ~ 4094 です。
root primary	このスイッチを強制的にルートスイッチに設定します。
root secondary	プライマリ ルートスイッチに障害が発生した場合に、このスイッチをルートスイッチに設定します。
diameter net-diameter	(任意) 2 つのエンドステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ~ 7 です。このキーワードは、MST インスタンス 0 の場合のみ使用できます。
hello-time seconds	(任意) ルートスイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔を設定します。指定できる範囲は 1 ~ 10 秒です。このキーワードは、MST インスタンス 0 の場合のみ使用できます。

デフォルト

プライマリ ルートスイッチのプライオリティは 24576 です。
セカンダリ ルートスイッチのプライオリティは 28672 です。
hello タイムは 2 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	<i>instance-id</i> の範囲が 1 ~ 4094 に変更されました。

使用上のガイドライン

spanning-tree mst instance-id 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 mst instance-id root コマンドを入力すると、ソフトウェアはこのスイッチをスパニングツリー インスタンスのルートに設定するのに十分なプライオリティを設定しようとします。拡張システム ID がサポートされているため、スイッチはインスタンスのスイッチプライオリティを 24576 に設定します (この値によってこのスイッチが指定されたインスタンスのルートになる場合)。指定インスタンスのルートスイッチに、24576 に満たないスイッチプライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチプライオリティより 4096 小さい値に設定します (4096 は 4 ビットスイッチプライオリティの最下位ビットの値です)。

spanning-tree mst instance-id root secondary コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアによりスイッチ プライオリティがデフォルト値 (32768) から 28672 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 (ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティ 32768 を使用しているためにルート スイッチになる可能性が低い場合)。

例

次の例では、スイッチをインスタンス 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 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

次の例では、スイッチをインスタンス 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 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree mst instance-id** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst instance-id	指定インスタンスの MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree port-priority

インターフェイス プライオリティを設定するには、**spanning-tree port-priority** 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。ループが発生した場合、スパンニング ツリーはフォワーディング ステートにするインターフェイスを判別できます。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。

spanning-tree [vlan *vlan-id*] port-priority *priority*

no spanning-tree [vlan *vlan-id*] port-priority

シンタックスの説明

vlan <i>vlan-id</i>	(任意) スパニングツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
<i>priority</i>	使用できる番号は 0 ~ 240 で、16 ずつ増加します。有効なプライオリティ値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

変数 *vlan-id* を省略した場合、このコマンドは VLAN 1 に関連付けられたスパンニングツリー インスタンスに適用されます。

インターフェイスが割り当てられていない VLAN にも、プライオリティを設定できます。このインターフェイスを VLAN に割り当てると、設定が有効になります。

インターフェイスを **spanning-tree vlan *vlan-id* port-priority *priority*** コマンドおよび **spanning-tree port-priority *priority*** コマンドを両方使用して設定する場合、**spanning-tree vlan *vlan-id* port-priority *priority*** コマンドが有効になります。

例

次の例では、ループが発生した場合にポートがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

次の例では、VLAN 20 ~ 25 のポート プライオリティ値を設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

設定を確認するには、**show spanning-tree interface *interface-id*** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface <i>interface-id</i>	特定のインターフェイスのスパニングツリー情報を表示します。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree portfast (グローバル コンフィギュレーション)

PortFast 対応のインターフェイス上で BPDU フィルタリングおよび BPDU ガード機能をグローバルにイネーブルにしたり、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにしたりするには、**spanning-tree portfast** 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。BPDU フィルタリング機能を使用すると、スイッチ インターフェイスでの BPDU の送受信を禁止できます。BPDU ガード機能は、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。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 {bpdufilter default | bpduguard default | default}

no spanning-tree portfast {bpdufilter default | bpduguard default | default}

シンタックスの説明	
bpdufilter default	PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにし、エンドステーションに接続されたスイッチ インターフェイスでの BPDU の送受信を禁止します。
bpduguard default	PortFast 対応インターフェイス上で BPDU ガード機能をグローバルにイネーブルにし、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。
default	すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。

デフォルト BPDU フィルタリング、BPDU ガード、および PortFast 機能は、個別に設定しないかぎり、すべてのインターフェイスでディセーブルです。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid PVST+ モード、または Multiple Spanning-Tree (MST) モードで稼動している場合は、これらの機能をイネーブルにできます。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドは、PortFast 対応インターフェイス (PortFast 動作ステートのインターフェイス) 上で BPDU フィルタリングをグローバルにイネーブルにします。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。スイッチ インターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

spanning-tree portfast bpdupfilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdupfilter** 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。

**注意**

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドは、PortFast 動作スタートのインターフェイス上で BPDU ガードをグローバルにイネーブルにします。有効な設定では、PortFast 対応インターフェイスは BPDU を受信しません。PortFast 対応インターフェイスが BPDU を受信した場合は、認可されていない装置の接続などのような無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは **errdisable** ステートになります。インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpduguard** 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。

すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast default** 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。PortFast は、エンドステーションに接続するインターフェイスに限って設定します。そうしないと、偶発的なトポロジ ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。リンクがアップすると、PortFast 対応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、ただちにスパニングツリーフォワーディング ステートに移行します。

spanning-tree portfast default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree portfast** 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。**no spanning-tree portfast default** 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、**spanning-tree portfast** 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個別に設定した場合を除き、すべてのインターフェイス上で PortFast をディセーブルにすることができます。

例

次の例では、BPDU フィルタリング機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast bpdupfilter default
```

次の例では、BPDU ガード機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast bpduguard default
```

次の例では、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast default
```

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。

関連コマンド

コマンド	説明
<code>show running-config</code>	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
<code>spanning-tree bpdupfilter</code>	インターフェイスが BPDU を送受信しないようにします。
<code>spanning-tree bpduguard</code>	BPDU を受信したインターフェイスを、errdisable ステートにします。
<code>spanning-tree portfast (インターフェイス コンフィギュレーション)</code>	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。

spanning-tree portfast (インターフェイス コンフィギュレーション)

対応するすべての VLAN 内の特定のインターフェイス上で PortFast 機能をイネーブルにするには、**spanning-tree portfast** 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。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。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。

spanning-tree portfast [disable | trunk]

no spanning-tree portfast

シンタックスの説明

disable	(任意) 指定されたインターフェイスの PortFast 機能をディセーブルにします。
trunk	(任意) トランキング インターフェイスの PortFast 機能をイネーブルにします。

デフォルト

すべてのインターフェイスで PortFast 機能はディセーブルですが、ダイナミック アクセス ポートでは自動的にイネーブルになります。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

この機能は、エンドステーションに接続するインターフェイスに限って使用します。そうしないと、偶発的なトポロジープが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** 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必要があります。**spanning-tree portfast** コマンドは、トランク ポートではサポートされません。

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid PVST+ モード、または Multiple Spanning-Tree (MST) モードで稼働している場合は、その機能をイネーブルにできます。

この機能はインターフェイス上のすべての VLAN に影響します。

PortFast 機能がイネーブルに設定されている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、ただちにスパニングツリー フォワーディング ステートに移行されます。

spanning-tree portfast default 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、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにできます。ただし、**spanning-tree portfast** 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、グローバル設定を上書きできます。

spanning-tree portfast default グローバル コンフィギュレーション コマンドを設定する場合は、**spanning-tree portfast disable** 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、トランク インターフェイス以外のインターフェイス上で PortFast 機能をイネーブルにできます。

spanning-tree portfast (インターフェイス コンフィギュレーション)

例

次の例では、特定のポート上で PortFast 機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

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。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」> 「File Management Commands」> 「Configuration File Management Commands」を選択してください。
spanning-tree bpdufilter	インターフェイスでのブリッジプロトコルデータユニット (BPDU) の送受信を禁止します。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree portfast (グローバル コンフィギュレーション)	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。

spanning-tree transmit hold-count

毎秒送信するブリッジプロトコル データ ユニット (BPDU) の数を設定するには、**spanning-tree transmit hold-count** 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。

spanning-tree transmit hold-count *[value]*

no spanning-tree transmit hold-count *[value]*

シンタックスの説明	<i>value</i>	(任意) 毎秒送信される BPDU 数。指定できる範囲は 1 ~ 20 です。
-----------	--------------	---

デフォルト	デフォルト値は 6 です。
-------	---------------

コマンド モード	グローバル コンフィギュレーション
----------	-------------------

コマンドの履歴	リリース	変更内容
	12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン	スイッチが Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) モードの場合、伝送ホールド カウント値が増加すると、CPU の使用率に大きく影響する可能性があります。この値を減らすと、コンバージェンスの速度が低下します。デフォルト設定を使用することを推奨します。
------------	---

例	次の例では、伝送ホールド カウントを 8 に設定する方法を示します。 <pre>Switch(config)# spanning-tree transmit hold-count 8</pre> 設定を確認するには、 show spanning-tree mst 特権 EXEC コマンドを入力します。
---	--

関連コマンド	コマンド	説明
	show spanning-tree mst	伝送ホールド カウントを含む、Multiple Spanning-Tree (MST) のリージョン設定およびステータスを表示します。

spanning-tree uplinkfast

リンクやスイッチに障害が発生した場合またはスパンニングツリーが自動的に再設定された場合に新しいルートポートを短時間で選択できるようにするには、**spanning-tree uplinkfast** 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。

spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

シンタックスの説明

max-update-rate <i>pkts-per-second</i>	(任意) 更新パケットを送信するときの 1 秒間のパケット数です。指定できる範囲は 0 ~ 32000 です。
---	---

デフォルト

UplinkFast はディセーブルです。
更新速度は 150 パケット/秒です。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、アクセス スイッチ上で使用します。

UplinkFast 機能は、Rapid PVST+ または Multiple Spanning-Tree (MST) モード用に設定できますが、スパンニングツリー モードを PVST+ に変更するまでこの機能はディセーブル (非アクティブ) のままです。

UplinkFast をイネーブルにすると、スイッチ全体に対してイネーブルになり、VLAN 単位でイネーブルにすることはできません。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティが 49152 に設定されます。UplinkFast をイネーブルにした場合または UplinkFast がすでにイネーブルになっている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスと VLAN トランクのパス コストが 3000 だけ増加します (パス コストを 3000 以上の値に変更した場合、パス コストは変更されません)。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低下します。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

ルートポートに障害が発生していることがスパンニング ツリーで検出されると、UplinkFast はスイッチをただちに代替ルートポートに変更して、新しいルートポートを直接フォワーディング ステートに移行させます。この間、トポロジ変更通知が送信されます。

UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロッキング ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが **root-inconsistent**（ブロック）になり、フォワーディング ステートに移行できなくなります。

max-update-rate を 0 に設定すると、ステーションを学習するフレームが生成されず、接続の切断後、スパニングツリー トポロジのコンバージェンスに要する時間が長くなります。

例

次の例では、UplinkFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree uplinkfast
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニングツリー インターフェイス ステートのサマリーを表示します。
spanning-tree vlan root primary	このスイッチを強制的にルート スイッチに設定します。

spanning-tree vlan

VLAN 単位でスパニングツリーを設定するには、**spanning-tree vlan** 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。

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time seconds | max-age seconds |
priority priority | root {primary | secondary} [diameter net-diameter
[hello-time seconds]]]
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | root]
```

シンタックスの説明

<i>vlan-id</i>	スパニングツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ~ 4094 です。
forward-time <i>seconds</i>	(任意) 指定したスパニングツリー インスタンスの転送遅延時間を設定します。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を指定します。指定できる範囲は 4 ~ 30 秒です。
hello-time <i>seconds</i>	(任意) ルート スイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔を設定します。指定できる範囲は 1 ~ 10 秒です。
max-age <i>seconds</i>	(任意) スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。スイッチがこのインターバル内にルート スイッチから BPDU メッセージを受信しない場合は、スパニングツリー トポロジが再計算されます。指定できる範囲は 6 ~ 40 秒です。
priority <i>priority</i>	(任意) 指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。この設定は、このスイッチがルート スイッチとして選択される可能性に影響します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ~ 61440 であり、刻み幅は 4096 です。有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。それ以外の値はすべて拒否されます。
root primary	(任意) このスイッチを強制的にルート スイッチに設定します。
root secondary	(任意) プライマリ ルート スイッチに障害が発生した場合に、このスイッチをルート スイッチに設定します。
diameter <i>net-diameter</i>	(任意) 2 つのエンド ステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ~ 7 です。

デフォルト

すべての VLAN でスパニング ツリーがイネーブルです。

転送遅延時間は 15 秒です。

hello タイムは 2 秒です。

有効期限は 20 秒です。

プライマリ ルート スイッチのプライオリティは 24576 です。

セカンダリ ルート スイッチのプライオリティは 28672 です。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

STP をディセーブルにすると、VLAN はスパンニングツリー トポロジへの参加を停止します。管理上のダウン状態のインターフェイスは、ダウン状態のままです。受信された BPDU は、他のマルチキャスト フレームと同様に転送されます。STP がディセーブルの場合、VLAN はループの検出や禁止を行いません。

現在アクティブではない VLAN 上で STP をディセーブルにしたり、変更を確認するには、**show running-config** または **show spanning-tree vlan vlan-id** 特権 EXEC コマンドを使用します。設定は、VLAN がアクティブである場合に有効となります。

STP をディセーブルにするか、再びイネーブルにすると、ディセーブルまたはイネーブルにする VLAN 範囲を指定できます。

VLAN をディセーブルにしてからイネーブルにした場合、その VLAN に割り当てられていたすべての VLAN は引き続きメンバーとなります。ただし、すべてのスパンニングツリー ブリッジ パラメータは元の設定 (VLAN がディセーブルになる直前の設定) に戻ります。

インターフェイスが割り当てられていない VLAN 上で、スパンニングツリー オプションをイネーブルにすることができます。インターフェイスに設定を割り当てると、設定が有効になります。

max-age seconds を設定すると、指定されたインターバル内にスイッチがルート スイッチから BPDU を受信しなかった場合に、スパンニングツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree vlan vlan-id 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 vlan vlan-id root コマンドを入力すると、ソフトウェアは各 VLAN の現在のルート スイッチのスイッチ プライオリティを確認します。拡張システム ID がサポートされているため、スイッチは指定された VLAN のスイッチ プライオリティを 24576 に設定します。これは、この値によってこのスイッチが指定された VLAN のルートになる場合です。指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します (4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です)。

spanning-tree vlan vlan-id root secondary コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアによりスイッチ プライオリティがデフォルト値 (32768) から 28672 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 (ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティ 32768 を使用しているためにルート スイッチになる可能性が低い場合)。

例

次の例では、VLAN 5 上で STP をディセーブルにする方法を示します。

```
Switch(config)# no spanning-tree vlan 5
```

設定を確認するには、**show spanning-tree** 特権 EXEC コマンドを入力します。このインスタンスのリストに、VLAN 5 は表示されません。

次の例では、VLAN 20 と VLAN 25 のスパンニングツリーについて、転送時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

次の例では、VLAN 20 ~ 24 のスパニングツリーについて、hello 遅延時間を 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

次の例では、VLAN 20 のスパニングツリーについて、有効期限を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

次の例では、スパニングツリー インスタンス 100 およびインスタンス 105 ~ 108 の **max-age** パラメータをデフォルト値に戻す方法を示します。

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

次の例では、VLAN 20 のスパニングツリーについて、プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

次の例では、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 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

次の例では、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 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree vlan *vlan-id*** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree vlan	スパニングツリー情報を表示します。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree guard	選択されたインターフェイスに対応するすべての VLAN に対して、ルート ガード機能またはループ ガード機能をイネーブルにします。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree portfast (グローバル コンフィギュレーション)	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast (インターフェイス コンフィギュレーション)	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。
spanning-tree uplinkfast	UplinkFast 機能をイネーブルにし、新しいルート ポートを短時間で選択できるようにします。

speed

10/100 Mb/s ポートまたは 10/100/1000 Mb/s ポートの速度を指定するには、**speed** 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。ポートをデフォルト値に戻すには、このコマンドの **no** または **default** 形式を使用します。

```
speed {10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate}
```

```
no speed
```

シンタックスの説明

10	ポートは 10 Mb/s で稼働します。
100	ポートは 100 Mb/s で稼働します。
1000	ポートは 1000 Mb/s で稼働します。このオプションは、10/100/1000 Mb/s ポートでのみ有効であり、これらのポート上にもみ表示されます。
auto	ポートが自動的に、もう一方のリンクの終端ポートを基準にして速度を検出します。 10 、 100 、または 1000 キーワードと auto キーワードを一緒に使用する場合、ポートは指定した速度で自動ネゴシエーションだけを行います。
nonegotiate	自動ネゴシエーションがディセーブルになり、ポートが 1000 Mb/s で稼働します (1000BASE-T SFP は nonegotiate キーワードをサポートしていません)。

デフォルト

デフォルトの設定は **auto** です。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 SFP モジュール ポートが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。

速度が **auto** に設定されている場合、スイッチはリンクの反対側の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を使用することを強く推奨します。インターフェイス 1 つが自動ネゴシエーションをサポートし、相手側がサポートしない場合、サポート側は **auto** 設定を使用しますが、相手側にデュプレックスおよび速度を設定します。



注意

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、再度イネーブルになる場合があります。

スイッチの速度パラメータとデュプレックス パラメータの設定に関する注意事項については、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 Interface Characteristics」の章を参照してください。

例

次の例では、ポートの速度を 100 Mbps に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed 100
```

次の例では、10 Mb/s でだけポートが自動ネゴシエートするように設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10
```

次の例では、10 Mb/s または 100 Mb/s でだけポートが自動ネゴシエートするように設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10 100
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
duplex	デュプレックス モードの動作を指定します。
show interfaces	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に対する統計情報を表示します。

srr-queue bandwidth limit

ポートの最大出力を制限するには、**srr-queue bandwidth limit** 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。

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

weight1 制限されるポート速度のパーセント。指定できる範囲は 10 ~ 90 です。

デフォルト

ポートはレート制限されておらず、100% に設定されます。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ライン レートは接続速度の 80% に下がります。ただし、ハードウェアはライン レートが 6 つずつ増加するよう調整しているので、この値は厳密ではありません。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの QoS (Quality of Service) ソリューションを満たさないと判断した場合のみ、設定を変更することができます。

例

次の例では、ポートを 800 Mb/s に制限する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

設定を確認するには、**show mls qos interface [interface-id] queuing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos srr-queue output cos-map	サービス クラス (CoS) 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface queueing	QoS 情報を表示します。
srr-queue bandwidth shape	シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅のシェーピングをイネーブルにします。
srr-queue bandwidth share	共有ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

srr-queue bandwidth shape

シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅のシェーピングをイネーブルにするには、**srr-queue bandwidth shape** 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。

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*

no srr-queue bandwidth shape



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>weight1 weight2</i>	シェーピングされるポートのパーセントを判別する重みを指定します。イン
<i>weight3 weight4</i>	バース比 ($1/weight$) は、このキューのシェーピング帯域幅を指定します。各
	値はスペースで区切ります。指定できる範囲は 0 ~ 65535 です。

デフォルト

ウェイト 1 は 25 に設定されています。ウェイト 2、ウェイト 3、および ウェイト 4 は 0 に設定されており、これらのキューは共有モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

シェーピング モードでは、キューは帯域幅のパーセントとして保証され、この量にレート制限されません。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を越えて使用できません。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。

シェーピング モードは、共有モードを無効にします。

srr-queue bandwidth shape 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シェーピングされたキューの重みを 0 に設定すると、このキューは共有モードに参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。

同じポートのキューにシェーピングと共有を混在させて設定する場合、最小のキューをシェーピングに設定します。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

例

次の例では、同じポートのキューをシェーピングと共有両方に設定する方法を示します。キュー 2、3、4 の重み比が 0 に設定されているので、キューは共有モードで動作します。キューの帯域幅の重みは 1/8、12.5% です。キュー 1 は、この帯域幅で保証され制限されています。他のキューにトラフィックがなくアイドルであっても、他のキューにスロットを拡張しません。キュー 2、3、4 は共有モードで、キュー 1 の設定は無視されます。共有モードのキューに割り当てられた帯域幅比は、4/ (4+4+4)、33% です。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

設定を確認するには、**show mls qos interface [interface-id] queuing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos srr-queue output cos-map	サービス クラス (CoS) 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) しきい値を設定し、バッファの可用性を確保し、キューセットに対する最大メモリ割り当てを設定します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface queuing	QoS (Quality of Service) 情報を表示します。
srr-queue bandwidth share	共有ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

srr-queue bandwidth share

シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにするには、**srr-queue bandwidth share** 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。重み比は、Shaped Round Robin (SRR) スケジューラが各キューからパケットを取り出す周波数比です。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。

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>weight1 weight2 weight3 weight4</i>	<i>weight1</i> 、 <i>weight2</i> 、 <i>weight3</i> 、および <i>weight4</i> は、SRR スケジューラがパケットを取り出す周波数比を指定します。各値はスペースで区切ります。指定できる範囲は 1 ~ 255 です。
--	--

デフォルト

ウェイト 1、ウェイト 2、ウェイト 3 およびウェイト 4 は 25 に設定されています (各キューに帯域幅の 1/4 を割り当て)。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

各重みの絶対値は意味がないので、パラメータ比だけを使用します。

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、キューが空でリンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。

srr-queue bandwidth shape 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シェーピングされたキューの重みを 0 に設定すると、このキューは SRR 共有モードに参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。

同じポートのキューにシェーピングと共有を混在させて設定する場合、最小のキューをシェーピングに設定します。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

例

次の例では、出力ポートで稼動する SRR スケジューラの重みの比を設定する方法を示します。キュー 4 つを使用します。共有モードの各キューに割り当てられた帯域幅は $1/(1+2+3+4)$ 、 $2/(1+2+3+4)$ 、 $3/(1+2+3+4)$ 、および $4/(1+2+3+4)$ であり、キュー 1、2、3、および 4 に対してそれぞれ 10%、20%、30%、および 40% です。つまり、キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍になります。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

設定を確認するには、**show mls qos interface [interface-id] queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos srr-queue output cos-map	サービスクラス (CoS) 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point (DSCP) 値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop (WTD) しきい値を設定し、バッファの可用性を保証し、キューセットに対する最大メモリ割り当てを設定します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface queueing	QoS (Quality of Service) 情報を表示します。
srr-queue bandwidth shape	シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅のシェーピングをイネーブルにします。

storm-control

インターフェイス上でブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御をイネーブルにし、しきい値のレベルを設定するには、**storm-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。

```
storm-control {{broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}} | {action {shutdown | trap}}
```

```
no storm-control {{broadcast | multicast | unicast} level} | {action {shutdown | trap}}
```

シンタックスの説明

broadcast	インターフェイス上でブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイス上でマルチキャスト ストーム制御をイネーブルにします。
unicast	インターフェイス上でユニキャスト ストーム制御をイネーブルにします。
level level [level-low]	<p>上限および下限抑制レベルをポートの全帯域幅のパーセンテージとして指定します。</p> <ul style="list-style-type: none"> level : 上限抑制レベル (小数点以下第 2 位まで)。指定できる範囲は 0.00 ~ 100.00 です。指定した level の値に達した場合、ストーム パケットのフラッディングをブロックします。 level-low : (任意) 下限抑制レベル (小数点以下第 2 位まで)。指定できる範囲は 0.00 ~ 100.00 です。この値は、上限抑制値より小さいまたは等しい必要があります。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。
level bps bps [bps-low]	<p>上限および下限抑制レベルを、ポートで受信するトラフィックの速度 (ビット/秒) として指定します。</p> <ul style="list-style-type: none"> bps : 上限抑制レベル (小数点以下第 1 位まで)。指定できる範囲は 0.0 ~ 10000000000.0 です。指定した bps の値に達した場合、ストーム パケットのフラッディングをブロックします。 bps-low : (任意) 下限抑制レベル (小数点以下第 1 位まで)。指定できる範囲は 0.0 ~ 10000000000.0 です。この値は、上限抑制値に等しいまたは小さい必要があります。 <p>大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。</p>

level pps pps [pps-low]	<p>上限および下限抑制レベルを、ポートで受信するトラフィックの速度（パケット/秒）として指定します。</p> <ul style="list-style-type: none"> • pps : 上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ~ 10000000000.0 です。指定した pps の値に達した場合、ストーム パケットのフラグディングをブロックします。 • pps-low : (任意) 下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ~ 10000000000.0 です。この値は、上限抑制値に等しいまたは小さい必要があります。 <p>大きい数値のしきい値には、k、m、g などのメトリック サフィックスを使用できません。</p>
action { shutdown trap }	<p>ポートでストームが発生した場合にとられるアクション。デフォルトアクションは、トラフィックをフィルタし、SNMP（簡易ネットワーク管理プロトコル）トラップを送信しません。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • shutdown : ストームの間、ポートをディセーブルにします。 • trap : ストーム発生時に、SNMP トラップを送信します。

デフォルト

ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。デフォルトアクションは、トラフィックをフィルタし、SNMP トラップを送信しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ストーム制御抑制レベルは、ポートの全帯域幅のパーセンテージとして、トラフィックが受信される速度（1 秒あたりのパケット数、または 1 秒あたりのビット数）として入力できます。

全帯域幅のパーセンテージとして指定した場合、100% の抑制値は、指定したトラフィック タイプに制限が設定されていないことを意味します。**level 0 0** の値は、ポート上のすべてのブロードキャスト、マルチキャスト、ユニキャストトラフィックをブロックします。ストーム制御は、上限抑制レベルが 100% 未満の場合のみイネーブルになります。他のストーム制御設定が指定されていない場合、デフォルトアクションは、ストームの原因となっているトラフィックをフィルタし、SNMP トラップを送信しません。



(注)

マルチキャストトラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータユニット (BPDU) および Cisco Discovery Protocol (CDP) フレームなどのコントロールトラフィック以外のマルチキャストトラフィックすべてがブロックされます。

trap および **shutdown** オプションは、互いに独立しています。

パケット ストームが検出されたときにシャットダウンを行う（ストームの間、ポートが `errdisable` になる）ようにアクションを設定する場合、インターフェイスをこのステートから解除するには **no shutdown** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**shutdown** アクションを指定しない場合、**trap**（ストーム検出時にスイッチがトラップを生成する）として指定してください。

ストームが発生し、実行されるアクションがトラフィックのフィルタリングである場合、下限抑制レベルが指定されていないと、トラフィック レートが上限抑制レベルより低くなるまでスイッチはすべてのトラフィックをブロックします。下限抑制レベルが指定されている場合、トラフィック レートがこのレベルより低くなるまでスイッチはトラフィックをブロックします。



(注)

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ブロードキャスト ストームが発生し、実行されるアクションがトラフィックのフィルタである場合、スイッチはブロードキャスト トラフィックのみをブロックします。

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。

例

次の例では、75.5% の上限抑制レベルでブロードキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control broadcast level 75.5
```

次の例では、87% の上限抑制レベルと 65% の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control unicast level 87 65
```

次の例では、2000 パケット/秒の上限抑制レベルと 1000 パケット/秒の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

次の例では、ポートで **shutdown** アクションをイネーブルにする方法を示します。

```
Switch(config-if)# storm-control action shutdown
```

設定を確認するには、**show storm-control** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show storm-control	すべてのインターフェイス上、または指定のインターフェイス上で、ブロードキャスト、マルチキャストまたはユニキャスト ストーム制御の設定を表示します。

switchport access

ポートをスタティックアクセスポートまたはダイナミックアクセスポートとして設定するには、**switchport access** インターフェイス コンフィギュレーション コマンドを使用します。スイッチポートのモードが、**access** に設定されている場合、ポートは指定の VLAN のメンバーとして動作します。**dynamic** として設定されている場合、ポートは受信した着信パケットに基づいて、VLAN 割り当ての検出を開始します。アクセスモードをスイッチのデフォルト VLAN 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 | dynamic}

no switchport access vlan

シンタックスの説明

vlan vlan-id	インターフェイスを、アクセスモード VLAN の VLAN ID を持つスタティックアクセスポートとして設定します。指定できる範囲は 1 ~ 4094 です。
vlan dynamic	VLAN メンバシップポリシーサーバ (VMPS) プロトコルによってアクセスモード VLAN が決まるように指定します。ポートに接続されたホスト (複数可) の送信元 MAC (メディアアクセス制御) アドレスに基づいて、ポートが VLAN に割り当てられます。スイッチは受信された新しい MAC アドレスをすべて VMPS サーバに送信して、ダイナミックアクセスポートに割り当てる VLAN の名前を取得します。ポートにすでに VLAN が割り当てられていて、送信元が VMPS によって承認されている場合、スイッチはパケットを該当する VLAN に転送します。

デフォルト

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。

ダイナミックアクセスポートは最初は何の VLAN にも属さず、受信したパケットに基づいて割り当てを受信します。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

switchport access vlan コマンドを有効にするには、ポートをアクセスモードにする必要があります。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 のみです。

ポートをダイナミックとして設定するには、事前に VMPS サーバ (Catalyst 6000 シリーズスイッチなど) を設定する必要があります。

ダイナミック アクセス ポートには、次の制限事項が適用されます。

- ソフトウェアでは、Catalyst 6000 シリーズ スイッチなどの VMPS をクエリーできる VLAN Query Protocol (VQP) クライアントが実装されます。Catalyst 2960 スイッチは、VMPS サーバではありません。ポートをダイナミックとして設定するには、事前に VMPS サーバを設定する必要があります。
- ダイナミック アクセス ポートは、エンドステーションを接続する場合のみ使用します。ブリッジングプロトコルを使用するスイッチまたはルータにダイナミック アクセス ポートを接続すると、接続が切断されることがあります。
- スパニングツリープロトコル (STP) がダイナミック アクセス ポートを STP ブロッキングステートにしないように、ネットワークを設定します。ダイナミック アクセス ポートでは、PortFast 機能が自動的にイネーブルになります。
- ダイナミック アクセス ポートは、1 つの VLAN にのみ属することができ、VLAN タギングは使用しません。
- ダイナミック アクセス ポートを次のように設定することはできません。
 - EtherChannel ポート グループのメンバー (ダイナミック アクセス ポートは、他のダイナミック ポートを含めて、他のポートとグループ化できません)
 - スタティック アドレス エントリ内の送信元または宛先ポート
 - モニタ ポート

例

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。

```
Switch(config-if)# switchport access vlan 2
```

設定を確認するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを入力して、Administrative Mode 行および Operational Mode 行の情報を調べます。

関連コマンド

コマンド	説明
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 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。
switchport mode	ポートの VLAN メンバシップ モードを設定します。

switchport backup interface

1 組のインターフェイスで相互にバックアップを提供する Flex Link を設定するには、レイヤ 2 インターフェイス上で **switchport backup interface** 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。Flex Link 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。

```
switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id |
Port-channel interface-id | TenGigabitEthernet interface-id ] {mmu primary vlan
interface-id | multicast fast-convergence | preemption {delay delay-time | mode} |
prefer vlan vlan-id}
```

```
no switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id
| Port-channel interface-id | TenGigabitEthernet interface-id ] {mmu primary vlan
interface-id | multicast fast-convergence | preemption {delay delay-time | mode} |
prefer vlan vlan-id}
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

FastEthernet	ファスト イーサネット IEEE 802.3 ポート名。指定できる範囲は 0 ~ 9 です。
GigabitEthernet	ギガビット イーサネット IEEE 802.3z ポート名。指定できる範囲は 0 ~ 9 です。
Port-channel	インターフェイスのイーサネット チャンネル。指定できる範囲は 0 ~ 48 です。
TenGigabitEthernet interface-id	10 ギガビット イーサネット ポート名。指定できる範囲は 0 ~ 9 です。 設定されるインターフェイスへのバックアップ リンクとしてレイヤ 2 インターフェイスが機能するように指定します。このインターフェイスには物理インターフェイスまたはポート チャンネルを指定できます。ポート チャンネル範囲は 1 ~ 486 です。
mmu	MAC アドレス移行更新。バックアップ インターフェイス ペアの Mac Move Update (MMU) を設定します。
primary vlan vlan-id	プライマリ VLAN となるプライベート VLAN の VLAN ID。指定できる範囲は 1 ~ 4,094 です。
multicast fast-convergence	マルチキャスト ファストコンバージェンス パラメータ。
preemption	バックアップ インターフェイス ペアのプリエンプション スキームを設定します。
delay delay-time	(任意) プリエンプション遅延を指定します。指定できる範囲は、1 ~ 300 秒です。
mode	プリエンプション モードを bandwidth 、 forced 、または off に設定します。
prefer vlan vlan-id	VLAN が Flex Link ペアのバックアップ インターフェイスで実行されるように指定します。VLAN ID 範囲は 1 ~ 4,094 です。
off	(任意) バックアップからアクティブへ移行する際、プリエンプションを行わないように指定します。
delay delay-time	(任意) プリエンプション遅延を指定します。指定できる範囲は、1 ~ 300 秒です。

デフォルト

デフォルトは、Flex Link が定義されていません。プリエンブション モードはオフです。プリエンブションを行いません。プリエンブション遅延は 35 秒に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SEE	preemption 、 mode 、 forced 、 bandwidth 、 off 、および delay キーワードが追加されました。
12.2(37)SE	prefer vlan キーワードが追加されました。
12.2(44)SE	multicast 、 fast-convergence 、 delay 、 mode 、 prefer 、および vlan キーワードが追加されました。

使用上のガイドライン

Flex Link を設定すると、1 つのリンクがプライマリ インターフェイスとして機能してトラフィックを転送し、もう一方のインターフェイスがスタンバイ モードになり、プライマリ リンクがシャットダウンされた場合に転送を開始できるように準備されます。設定されるインターフェイスはアクティブ リンクと呼ばれ、指定されたインターフェイスをバックアップ リンクとして識別されます。この機能はスパンニングツリー プロトコル (STP) の代わりに提供され、ユーザが STP をオフにした場合でも基本的なリンク冗長性を維持できます。

- このコマンドは、レイヤ 2 インターフェイスに対してのみ使用可能です。
- アクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つのアクティブ リンクに対してのみバックアップ リンクになれます。アクティブ リンクは別の Flex Link ペアに属することはできません。
- バックアップ リンクはアクティブ リンクと同じタイプ (たとえばファスト イーサネットやギガビット イーサネット) でなくてもかまいません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を似たような特性で設定する必要があります。
- いずれのリンクも EtherChannel に属するポートにはなれません。ただし、2 つのポート チャネル (EtherChannel 論理インターフェイス) を Flex Link として設定でき、ポート チャネルと物理インターフェイスを Flex Link として設定でき、ポート チャネルまたは物理インターフェイスをアクティブ リンクにできます。
- STP がスイッチに設定されている場合、Flex Link はすべての有効な VLAN で STP に参加しません。STP が動作していない場合、設定されているトポロジでループが発生していないことを確認してください。

例

次に、2 つのインターフェイスを Flex Link として設定する例を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end
```

次の例では、常にバックアップをプリエンプトするようにファストイーサネットインターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preempton forced
Switch(conf-if)# end
```

次の例では、ファストイーサネットインターフェイスのプリエンプション遅延時間を設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preempton delay 150
Switch(conf-if)# end
```

次の例では、MMU プライマリ VLAN としてファストイーサネットインターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

設定を確認するには、`show interfaces switchport backup` 特権 EXEC コマンドを入力します。

次の例では、優先 VLAN を設定する方法を示します。

```
Switch(config)# interface gigabitethernet 0/6
Switch(config-if)# switchport backup interface gigabitethernet 0/8 prefer vlan 60,100-120
```

設定を確認するには、`show interfaces switchport backup` 特権 EXEC コマンドを入力します。

この例では、VLAN 60、および 100 ~ 120 がスイッチに設定されています。

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、Gi0/6 が VLAN 1 ~ 50 のトラフィックを転送し、Gi0/8 が VLAN 60 および 100 ~ 120 のトラフィックを転送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Up/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると (LINK_DOWN)、このインターフェイスで優先される VLAN は Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi0/6 がダウンすると、Gi0/8 が Flex Link ペアのすべての VLAN を伝送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi0/6 がアップになって、このインターフェイスに指定されていた VLAN がピア インターフェイス Gi0/8 上でブロックされ、Gi0/6 に転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet0/6  GigabitEthernet0/8  Active Up/Backup Up
```

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

次の例では、インターフェイス Gi0/11 上でマルチキャスト ファストコンバージェンスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/11
Switch(config-if)# switchport backup interface gigabitEthernet 0/12 multicast
fast-convergence
Switch(config-if)# end
```

設定を確認するには、**show interfaces switchport backup detail** 特権 EXEC コマンドを入力します。

```
Switch# show interfaces switchport backup detail
```

```
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet0/11  GigabitEthernet0/12  Active Up/Backup Standby
Preemption Mode      : off
Multicast Fast Convergence : On
Bandwidth : 1000000 Kbit (Gi0/11), 1000000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

関連コマンド

コマンド	説明
show interfaces [<i>interface-id</i>] switchport backup	スイッチまたは指定されているインターフェイスに設定されている Flex Link とそのステータスを表示します。

switchport block

不明なマルチキャストまたはユニキャストのパケットが転送されないようにするには、**switchport block** 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。未知の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}

シンタックスの説明

multicast	不明なマルチキャストトラフィックをブロックするよう指定します。
unicast	不明なユニキャストトラフィックをブロックするよう指定します。

デフォルト

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。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、不明な MAC（メディアアクセス制御）アドレスを持った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はブロックすることができます。保護ポートで、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ブロックされない場合、セキュリティ上の問題が発生します。

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のブロックは、保護ポート上で自動的にイー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。

例

次の例では、インターフェイス上で不明なマルチキャストトラフィックをブロックする方法を示します。

```
Switch(config-if)# switchport block multicast
```

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。

関連コマンド

コマンド	説明
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。

switchport host

ホスト接続のためにポートを最適化するには、**switchport host** 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。システム上への影響をなくすには、このコマンドの **no** 形式を使用します。

switchport host

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートのデフォルトは、ホストへの接続が最適化されていません。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ホスト接続のためポートを最適化するには、**switchport host** コマンドでアクセスするスイッチ ポート モードを設定し、スパニング ツリー **PortFast** をイネーブルにし、チャンネル グルーピングをディセーブルにします。エンドステーションのみこの設定を適用することができます。

スパニング ツリー **PortFast** はイネーブルなので、**switchport host** コマンドを単一ホストと接続するポートにだけ入力します。その他のスイッチ、ハブ、コンセントレータ、またはブリッジと **fast-start** ポートを接続すると、一時的にスパニングツリー ループが発生することがあります。

switchport host コマンドをイネーブルにし、パケット転送の開始における遅延時間を減少させることができます。

例

次の例では、ポートのホスト接続の設定を最適化する方法を示します。

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

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。

関連コマンド

コマンド	説明
show interfaces switchport	スイッチポート モードを含む、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。

switchport mode

ポートの VLAN メンバシップ モードを設定するには、**switchport mode** 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。モードをデバイスの適切な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}
```

```
no switchport mode {access | dynamic | trunk}
```

シンタックスの説明

access	ポートをアクセス モード (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) に設定します。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のできるのは、1 つの VLAN のみです。
dynamic auto	インターフェイス トランキング モード 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	インターフェイス トランキング モード 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	無条件にポートをトランクに設定します。ポートは VLAN レイヤ 2 インターフェイスをトランキングします。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、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。

デフォルト

デフォルト モードは **dynamic auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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のみです。

access モードを入力した場合、インターフェイスは固定的な非トランキング モードになり、近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 モードを入力した場合、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現在の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 モードを入力した場合に、ネイバー インターフェイスが **trunk** または **desirable** モードに設定されると、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 モードを入力した場合に、ネイバー インターフェイスが **trunk**、**desirable**、または **auto** モードに設定されると、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 プロトコルであるダイナミック トランキング プロトコル (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。この事態を避けるには、DTP をサポートしない装置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、つまり DTP をオフにするように設定する必要があります。

- これらのリンクを介して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装置で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。

アクセス ポートとトランク ポートは、相互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と、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と、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 **dynamic auto** または **dynamic desirable** ポート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と、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。

例

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。

```
Switch(config)# interface gigabitethernet0/1
Switch(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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode dynamic desirable
```

次の例では、ポートを **trunk** モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

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、Administrative Mode 行および Operational Mode 行の情報を調べます。

関連コマンド

コマンド	説明
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。
switchport access	ポートをスタティックアクセスポートまたはダイナミックアクセスポートとして設定します。
switchport trunk	インターフェイスがトランクモードの場合、トランクの特性を設定します。

switchport nonegotiate

レイヤ 2 インターフェイス上でダイナミック トランキング プロトコル (DTP) ネゴシエーション パケットが送信されないように指定するには、**switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用します。スイッチは、このインターフェイス上で DTP ネゴシエーションを行いません。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。

switchport nonegotiate

no switchport nonegotiate

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

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。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

nonegotiate ステータスを解除するには、**switchport nonegotiate** コマンドの **no** 形式を使用します。

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) の場合のみです。**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、エラーが戻されます。

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。デバイスは、**mode** パラメータ (**access** または **trunk**) に従って、トランキングを実行するかどうかを決定します。

- これらのリンクを介して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で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。

■ switchport nonegotiate

例

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トを制限し、(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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport nonegotiate
```

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。

関連コマンド

コマンド	説明
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。
switchport mode	ポートの VLAN メンバシップモードを設定します。

switchport port-security

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には、キーワードなしで **switchport port-security** 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。キーワードを指定すると、セキュア MAC (メディア アクセス制御) アドレス、スティッキ MAC アドレス ラーニング、セキュア MAC アドレスの最大数、または違反モードが設定されます。ポートセキュリティをディセーブルにするか、またはパラメータをデフォルト状態に戻すには、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}}] |
  mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}]] [maximum value
  [vlan {vlan-list | {access | voice}}]]
```

```
no switchport port-security [mac-address mac-address [vlan {vlan-id | {access | voice}}] |
  mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}]] [maximum value
  [vlan {vlan-list | {access | voice}}]]
```

```
switchport port-security [aging] [violation {protect | restrict | shutdown | shutdown vlan}]
```

```
no switchport port-security [aging] [violation {protect | restrict | shutdown | shutdown
  vlan}]
```

シンタックスの説明

aging	(任意) switchport port-security aging コマンドを参照してください。
mac-address mac-address	(任意) 48 ビット MAC アドレスを入力して、インターフェイスのセキュア MAC アドレスを指定します。設定された最大値まで、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 ポート上でのみ、VLAN ID および MAC アドレスを指定します。VLAN ID が指定されない場合、ネイティブ VLAN が使用されます。
vlan access	(任意) アクセス ポートでのみ、VLAN をアクセス VLAN として指定します。
vlan voice	(任意) アクセス ポートでのみ、VLAN を音声 VLAN として指定します。 (注) voice キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合のみ利用可能です。
mac-address sticky [mac-address]	(任意) インターフェイスのスティッキ ラーニングをイネーブルにするには、 mac-address sticky キーワードのみを入力します。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され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。 (任意) <i>mac-address</i> を入力し、スティッキ セキュア MAC アドレスを指定します。

maximum value	<p>(任意) 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。スイッチで設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている MAC アドレスの最大数によって決まります。この数字は、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。</p> <p>デフォルトの設定は 1 です。</p>
vlan [vlan-list]	<p>(任意) トランク ポートに対して、VLAN のセキュア MAC アドレスの最大数を設定できます。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。</p> <ul style="list-style-type: none"> • vlan : VLAN ごとに最大値を設定します。 • vlan vlan-list : VLAN 範囲、または一連の VLAN 内の VLAN ごとに最大値を設定します。VLAN 範囲はハイフン、一連の VLAN はカンマで区切ります。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。
violation	<p>(任意) セキュリティ違反モード、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します。デフォルトは shutdown です。</p>
protect	<p>セキュリティ違反保護モードを設定します。このモードでは、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パケットはドロップされます。ドロップすることでセキュア MAC アドレス数を下げるか、許可するアドレスの最大数を増やさないかぎり、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。</p> <p>(注) 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、ポートが最大制限に達していても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。</p>
restrict	<p>セキュリティ違反制限モードを設定します。このモードでは、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パケットはドロップされます。ドロップすることでセキュア MAC アドレス数を下げるか、許可するアドレスの最大数を増やさないかぎり、この状態が続きます。SNMP トラップが送信されます。また、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。</p>
shutdown	<p>セキュリティ違反シャットダウン モードを設定します。このモードでは、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 の状態になります。SNMP トラップが送信されます。また、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したり、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 コマンドを入力したりして、手動で再びイネーブルにすることができます。</p>
shutdown vlan	<p>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。このモードでは、違反が発生した VLAN のみが errdisable になります。</p>

デフォルト

ポート セキュリティはディセーブルです。

ポート セキュリティがイネーブルであり、キーワードが入力されていない場合、セキュア MAC アドレスの最大数のデフォルト値は 1 です。

デフォルトの違反モードは、**shutdown** です。

スティッキ ラーニングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(35)SE	shutdown vlan キーワードが追加されました。

使用上のガイドライン

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 Fast EtherChannel または Gigabit 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 に設定する必要があります。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 つを許可する十分なセキュア アドレスを設定する必要があります。
- 音声 VLAN はアクセス ポート上のみでサポートされます。トランク ポート上ではサポートされません。
- インターフェイスにセキュア アドレス最大値を入力した場合、新規の値が前回の値より大きいと、新規の値により、前回の設定値が無効にされます。新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングはサポートしていません。

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 アドレスのステーションがインターフェイスにアクセスしようとする場合、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 アドレスを持ったステーションがインターフェイスにアクセスしようとする場合、セキュリティ違反が起きます。

セキュアポートが `errdisable` ステートになっているときは、**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 shut down** 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。

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。

最大セキュア アドレスの値をインターフェイスに入力した場合、次の事象が発生します。

- 新しい値が古い値より大きい場合、新しい値が古い設定値を上書きします。
- 新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。

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、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 アドレスを（スティッキ ラーニングがイネーブルになる前にダイナミックに学習されたアドレスも含め）、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か、または実行コンフィギュレーションを削除する場合、スティッキ セキュア MAC アドレスの一部は実行コンフィギュレーションのままですが、アドレス テーブルから削除されます。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、アドレスはアドレス テーブルと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、スイッチの再起動時、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 アドレスが保存されていない場合は、アドレスは失われます。スティッキ ラーニングをディセーブルにした場合、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。
- スティッキ 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追加されません。

例

次の例では、ポート上でポート 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。違反モードがデフォルト モードであり、セキュア MAC アドレスが設定されていません。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

次の例では、ポート上でセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキ ラーニングをイネーブルにして、ポート上で2つのスティッキ セキュア MAC アドレスを入力する方法を示します。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

次の例では、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にポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config)# switchport port-security violation shutdown vlan
```

設定を確認するには、**show port-security** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからスイッチ上またはインターフェイス上の特定のタイプのセキュア アドレスまたはすべてのセキュア アドレスを削除します。
show port-security address	スイッチで設定されるすべてのセキュア アドレスを表示します。
show port-security interface interface-id	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を表示します。

switchport port-security aging

セキュア アドレス エントリのエージング タイムとタイプを設定したり、特定のポート上でのセキュア アドレスのエージング動作を変更したりするには、**switchport port-security aging** 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。ポート セキュリティのエージングをディセーブルにしたり、パラメータをデフォルト状態に戻したりする場合は、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}

シンタックスの説明

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。 time 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 time (分) が経過したあとに期限切れとなり、セキュア アドレス リストから削除されます。
inactivity	非アクティブティ エージング タイプを設定します。指定された time 期間中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。

デフォルト

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。デフォルト期間は 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。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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、**no switchport 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。

例

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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

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をイネーブルにし、**inactivity** タイプのエージングでエージング タイムを 2 分に設定します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュア アドレスに対してエージングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport port-security aging static
```

関連コマンド

コマンド	説明
show port-security	ポートに定義されたポート セキュリティ設定を表示します。
switchport port-security	ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。

switchport priority extend

着信タグなしフレームのポート プライオリティを設定したり、指定のポートに接続された IP Phone が受信するフレームのプライオリティを設定したりするには、**switchport priority extend** 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 priority extend {cos value | trust}

no switchport priority extend



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

cos value	PC から受信したか、または特定のサービス クラス (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になります。デフォルト値は 0 です。
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。

デフォルト

ポートで受信したタグのないフレームについて、デフォルト ポート プライオリティは、CoS 値 0 に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

音声 VLAN をイネーブルにした場合、スイッチを設定して、Cisco Discovery Protocol (CDP) パケットを送信し、Cisco IP Phone のアクセス ポートに接続する装置からデータ パケットを送信する方法を IP Phone に指示できます。Cisco IP Phone に設定を送信するには、Cisco IP Phone に接続するスイッチ ポートの CDP をイネーブルする必要があります (デフォルトにより、CDP はすべてのスイッチ インターフェイスでグローバルにイネーブルです)。

スイッチ アクセス ポート上で音声 VLAN を設定する必要があります。

音声 VLAN をイネーブルにする前に、**mls qos** 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スイッチの QoS (Quality of Service) をイネーブルにし、**mls qos trust cos** 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、信頼するポート信頼状態を設定することを推奨します。

例 次の例では、受信された 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。

```
Switch(config)# interface gigabitethernet0/2  
Switch(config-if)# switchport priority extend trust
```

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。

関連コマンド

コマンド	説明
show interfaces	スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport voice vlan {vlan-id dot1p none untagged}	ポートに音声 VLAN を設定します。

switchport protected

同じスイッチ上で保護された他のポートから送信されるレイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離するには、**switchport protected** 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。ポートで保護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。

switchport protected

no switchport protected

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

保護ポートは定義されていません。すべてのポートが保護されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチポート保護機能はスイッチに対してローカルです。同じスイッチ上の保護ポート間の通信は、レイヤ 3 デバイスを通してのみ行うことができます。異なるスイッチ上の保護ポート間の通信を禁止するには、各スイッチの保護ポートに一意の VLAN を設定し、スイッチ間にトランク リンクを設定する必要があります。保護ポートはセキュア ポートとは異なります。

保護ポートは、他の保護ポートにユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、PIM パケットなどの制御トラフィックのみが転送されます。保護ポート間を通過するすべてのデータ トラフィックはレイヤ 3 装置を介して転送されなければなりません。

モニタするポートおよびモニタされるポートの両方が保護ポートの場合、ポート モニタリングは機能しません。

例

次の例では、インターフェイス上で保護ポートをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport protected
```

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。

シンタックスの説明	コマンド	説明
	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 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。
	switchport block	インターフェイス上で不明なユニキャストまたはマルチキャストトラフィックを防ぎます。

switchport trunk

インターフェイスがトランキング モードの場合にトランクの特性を設定するには、**switchport trunk** 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。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**}}

シンタックスの説明

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。次の <i>vlan-list</i> 形式を参照してください。 none キーワードは無効です。デフォルトは all です。
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。 all キーワードは無効です。

vlan-list の形式は、**all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [,*vlan-atom*...] です。各キーワードの意味は、次のとおりです。

- **all** は 1 ~ 4094 のすべての VLAN を示します。このキーワードは、リスト内のすべての VLAN を同時に設定することを許可していないコマンドでは使用できません。
- **none** は空のリストを意味します。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** は現在設定されている VLAN リストを置き換えないで、定義済み VLAN 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 ID (VLAN ID が 1005 より上) を使用できます。



(注) 拡張範囲 VLAN は許可 VLAN リストには追加できますが、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。指定の範囲の ID に対してはハイフンを使用します。

- **remove** は現在設定されている VLAN リストを置き換えないで、リストから定義済み VLAN 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。



(注) 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。

カンマを使い、連続しない VLAN ID を区切ります。指定の範囲の ID に対してはハイフンを使用します。

- **except** は定義済み VLAN リスト以外の、計算する必要がある VLAN を示します（指定した VLAN を除く VLAN が追加されます）。有効な ID は 1 ～ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。指定の範囲の ID に対して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、より小さい値が最初になります（ハイフン区切り）。

デフォルト

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。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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危険性を減らすには、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 をディセーブルにします。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]、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 ポートにだけ適用されます。
- 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、フラグディング 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。

例

次の例では、VLAN 3 を、すべてのタグなしトラフィックを送信するデフォルト ポートに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(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。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーン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。

```
Switch(config)# interface gigabitethernet0/2
Switch(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。

関連コマンド

コマンド	説明
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。
switchport mode	ポートの VLAN メンバシップモードを設定します。

switchport voice vlan

ポートに音声 VLAN を設定するには、**switchport voice vlan interface** 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 voice vlan {vlan-id | dot1p | none | untagged}
```

```
no switchport voice vlan
```

シンタックスの説明

vlan-id	音声トラフィックに VLAN を使用するように設定します。指定できる範囲は 1 ~ 4094 です。デフォルトでは、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	IP Phone をタグなしの音声トラフィックを送信するように設定します。これが IP Phone のデフォルト設定になります。

デフォルト

デフォルトでは、スイッチは 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。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

スイッチの Cisco IP Phone に接続しているスイッチポート上の Cisco Discovery Protocol (CDP; シスコ検出プロトコル) をイネーブルにし、Cisco IP Phone に設定情報を送信する必要があります。インターフェイス上で CDP は、デフォルトの状態グローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**mls qos** 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スイッチの QoS (Quality of Service) をイネーブルにし、**mls qos trust cos** 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、信頼するポート信頼状態を設定することを推奨します。

VLAN ID を入力すると、IP Phone は指定された VLAN ID のタグが付けられた音声トラフィックを IEEE 802.1Q フレームで転送します。スイッチは 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、スイッチ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 値を選びます。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 に設定する必要があります。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 つを許可する十分なセキュア 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 では、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。

例 次の例では、VLAN 2 をポート用音声 VLAN として設定します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport voice vlan 2
```

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。

関連コマンド

コマンド	説明
show interfaces interface-id switchport	スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport priority extend	指定されたポートに接続されたデバイスが、着信ポートで受信したプライオリティ トラフィックを処理する方法を指定します。

system mtu

ギガビットイーサネットポートまたはファストイーサネット (10/100) ポートの最大パケットサイズや最大伝送ユニット (MTU) サイズを設定するには、**system mtu** 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。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 | jumbo bytes}
```

```
no system mtu
```

シンタックスの説明

<i>bytes</i>	10 Mb/s または 100 Mb/s に設定されているポートのシステム MTU を設定します。指定できる範囲は 1500 ~ 1998 バイトです。これは、10/100 Mbps イーサネット スイッチ ポートで受信される最大 MTU です。
<i>jumbo bytes</i>	1000 Mbps 以上で稼動しているギガビットイーサネットポートのシステムジャンボ MTU を設定します。指定できる範囲は 1500 ~ 9000 バイトです。これは、ギガビットイーサネットポートの物理ポートで受信される最大 MTU です。

デフォルト

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。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドでシステム MTU またはジャンボ MTU のサイズを変更した場合、新しい設定内容を反映させるには、スイッチをリセットする必要があります。システム MTU 設定は、NVRAM のスイッチ環境変数に保存され、スイッチがリロードした時点で有効になります。**system mtu** コマンドおよび **system mtu jumbo** コマンドで入力した MTU 設定は、**copy running-config startup-config** 特権 EXEC コマンドを入力しても、スイッチ IOS コンフィギュレーションファイルに保存されません。したがって、TFTP を使用し、バックアップ コンフィギュレーションファイルで新しいスイッチを設定して、システム MTU をデフォルト以外の値にしたい場合、新しいスイッチ上で **system mtu** および **system mtu jumbo** を明示的に設定し、スイッチをリロードする必要があります。

1000 Mbps で稼動しているギガビットイーサネットポートは **system mtu** コマンドによる影響を受けません。10/100 Mbps ポートは **system mtu jumbo** コマンドによる影響を受けません。

指定されたスイッチタイプの許容範囲外の値を入力すると、値が拒否されます。



(注)

スイッチは、インターフェイスごとの MTU の設定をサポートしません。

system mtu

スイッチの CPU で受信できるフレーム サイズは、**system mtu** コマンドで入力した値に関係なく、1998 バイトに制限されています。転送されたフレームまたはルーテッドフレームは、通常 CPU では受信されませんが、一部の packets (制御トラフィック、SNMP、Telnet、およびルーティング プロトコルなど) は CPU に送信されます。

たとえば、**system mtu** 値が 1998 バイトであり、**system mtu jumbo** 値が 5000 バイトである場合、1000 Mb/s で稼働しているインターフェイスでは、最大 5000 バイトの packets を受信できます。ただし、1998 バイトを超える packets は 1000 Mb/s で稼働しているインターフェイスで受信できませんが、宛先インターフェイスが 10 Mb/s または 100 Mb/s で稼働している場合はドロップされます。

例

次の例では、1000 Mbps 以上で稼働しているギガビット イーサネット ポートの最大ジャンボ packet サイズを 1800 バイトに設定する方法を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

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。

関連コマンド

コマンド	説明
show system mtu	ファスト イーサネットおよびギガビット イーサネットのポートに設定された packet サイズを表示します。

test cable-diagnostics tdr

インターフェイス上で Time Domain Reflector (TDR) 機能を実行するには、**test cable-diagnostics tdr** 特権 EXEC コマンドを使用します。

test cable-diagnostics tdr interface *interface-id*

シンタックスの説明	<i>interface-id</i>	TDR を実行するインターフェイスを指定します。
-----------	---------------------	--------------------------

デフォルト	デフォルトはありません。	
-------	--------------	--

コマンドモード	特権 EXEC	
---------	---------	--

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。SFP モジュールポートではサポートされません。TDR の詳細については、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。

test cable-diagnostics tdr interface *interface-id* コマンドを使用して TDR を実行したあと、結果を表示するには **show cable-diagnostics tdr interface *interface-id*** 特権 EXEC 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 TDR を実行する方法を示します。

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

インターフェイスのリンク ステータスがアップであり、速度が 10 Mb/s または 100 Mb/s である場合、**test cable-diagnostics tdr interface *interface-id*** コマンドを入力すると次のメッセージが表示されま

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

関連コマンド	コマンド	説明
	show cable-diagnostics tdr	TDR 結果が表示されます。

tracertoute mac

指定された送信元 MAC アドレスから指定された宛先 MAC アドレスまでのパケットがたどるレイヤ 2 パスを表示するには、**tracertoute mac** 特権 EXEC コマンドを使用します。

```
tracertoute mac [interface interface-id] {source-mac-address} [interface interface-id]
  {destination-mac-address} [vlan vlan-id] [detail]
```

シンタックスの説明

interface <i>interface-id</i>	(任意) 送信元および宛先スイッチ上のインターフェイスを指定します。
source-mac-address	送信元スイッチの MAC アドレスを指定します (16 進数)。
<i>destination-mac-address</i>	宛先スイッチの MAC アドレスを指定します (16 進数)。
vlan <i>vlan-id</i>	(任意) 送信元スイッチから宛先スイッチを通過するパケットのレイヤ 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 は 1 ~ 4094 です。
detail	(任意) 詳細情報を表示するよう指定します。

デフォルト

デフォルトはありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 の **tracertoute** を適切に機能させるには、シスコ検出プロトコル (CDP) がネットワークのすべてのスイッチ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。

スイッチがパス内でレイヤ 2 **tracertoute** をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 **trace** クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 10 です。

レイヤ 2 **tracertoute** はユニキャスト トラフィックのみをサポートします。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の MAC アドレスが同じ VLAN にある場合、**tracertoute 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 MAC アドレスを指定しても、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 にある場合、送信元および宛先 MAC アドレス両方の属する VLAN を指定する必要があります。VLAN が指定されないと、パスは識別されず、エラー メッセージが表示されます。

複数のデバイスがハブを通じて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1つのポートで検知される場合）、レイヤ 2 traceroute の機能はサポートされません。1つのポートで複数の CDP ネイバーが検知される場合、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せん。

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。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5          ) :   Gi0/3 => Gi0/1
con1          (2.2.1.1          ) :   Gi0/1 => Gi0/2
con2          (2.2.2.2          ) :   Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用してレイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
C-12T / 2.2.6.6 :
    Gi0/2 [auto, auto] => Gi0/3 [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、送信元スイッチと宛先スイッチ上のインターフェイスを指定してレイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5          ) :   Gi0/3 => Gi0/1
con1          (2.2.1.1          ) :   Gi0/1 => Gi0/2
con2          (2.2.2.2          ) :   Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、該当するスイッチが送信元スイッチに接続されていない場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ....
Source 0000.0201.0501 found on con5[WS-C2960-12T] (2.2.5.5)
con5 / WS-C2960-12T / 2.2.5.5 :
    Gi0/1 [auto, auto] => Gi0/3 [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、該当するスイッチが送信元 MAC アドレス用の宛先ポートを検出できない場合のレイヤ 2 パスを示します。

```
Switch# tracertoute 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。

```
Switch# tracertoute 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。

```
Switch# tracertoute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

次の例では、送信元および宛先スイッチが複数の VLAN にある場合のレイヤ 2 のパスを示しています。

```
Switch# tracertoute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
tracertoute 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 パスを表示します。

traceroute mac ip

指定された送信元 IP アドレスまたはホスト名から指定された宛先 IP アドレスまたはホスト名までのパケットがたどるレイヤ 2 パスを表示するには、**traceroute mac ip** 特権 EXEC コマンドを使用します。

```
traceroute mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]
```

シンタックスの説明

<i>source-ip-address</i>	送信元スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
<i>destination-ip-address</i>	宛先スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
<i>source-hostname</i>	送信元スイッチの IP ホスト名を指定します。
<i>destination-hostname</i>	宛先スイッチの IP ホスト名を指定します。
detail	（任意）詳細情報を表示するよう指定します。

デフォルト

デフォルトはありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 の **traceroute** を適切に機能させるには、シスコ検出プロトコル（CDP）がネットワークのすべてのスイッチ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。

スイッチがパス内でレイヤ 2 **traceroute** をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 **trace** クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 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、**traceroute 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、スイッチはアドレス解決プロトコル（ARP）を使用し、IP アドレスとそれに対応する MAC（メディアアクセス制御）アドレスおよび VLAN ID を関連付けます。

- 指定の IP アドレスの ARP のエントリが存在していた場合、スイッチは関連付けられた 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、スイッチは ARP クエリーを送信し、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。

複数のデバイスがハブを通じて 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 1 つのポートで検知される場合）、レイヤ 2 `tracertoute` の機能はサポートされません。1 つのポートで複数の CDP ネイバーが検知される場合、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せん。

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、送信元および宛先 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。

```
Switch# tracertoute 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-C2960-12T / 2.2.6.6 :
    Gi0/1 [auto, auto] => Gi0/3 [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、送信元と宛先のホスト名を指定してレイヤ 2 パスを表示する方法を示します。

```
Switch# tracertoute 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) :Gi0/1 => Gi0/3
con5           (2.2.5.5       ) :   Gi0/3 => Gi0/1
con1           (2.2.1.1       ) :   Gi0/1 => Gi0/2
con2           (2.2.2.2       ) :   Gi0/2 => 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。

```
Switch# tracertoute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
<code>tracertoute mac</code>	指定された送信元 MAC アドレスから指定された宛先 MAC アドレスまでパケットがたどるレイヤ 2 パスを表示します。

trust

class ポリシー マップ コンフィギュレーション コマンドまたは **class-map** グローバル コンフィギュレーション コマンドで分類されたトラフィックの信頼状態を定義するには、**trust** 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。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。

```
trust [cos | dscp | ip-precedence]
```

```
no trust [cos | dscp | ip-precedence]
```

シンタックスの説明

cos	(任意) パケットのサービス クラス (CoS) 値を使用して、入力パケットを分類します。タグのないパケットの場合、デフォルト ポートの CoS 値が使用されます。
dscp	(任意) パケットの Differentiated Service Code Point (DSCP) 値 (8 ビット サービス タイプ フィールドの上位 6 ビット) を使用することにより、入力パケットを分類します。パケットにタグがある場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットにタグがない場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。
ip-precedence	(任意) パケットの IP precedence 値 (8 ビット サービスタイプ フィールドの上位 3 ビット) を使用して、入力パケットを分類します。パケットにタグがある場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットにタグがない場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。

デフォルト

信頼できない状態です。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。

コマンド モード

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

特定のトラフィックの QoS (Quality of Service) の信頼動作を他のトラフィックと区別するために、このコマンドを使用します。たとえば、ある DSCP 値を持った着信トラフィックが信頼されます。着信トラフィックの DSCP 値と一致し、信頼できるクラス マップを設定できます。

このコマンドで設定された信頼性の値は、**mls qos trust** インターフェイス コンフィギュレーション コマンドで設定された信頼性の値を上書きします。

trust コマンドは、同一ポリシー マップ内の **set** ポリシーマップ クラス コンフィギュレーション コマンドと相互に排他的な関係にあります。

trust cos を指定した場合、QoS は受信した、またはデフォルト ポートの CoS 値および CoS/DSCP マップを使用し、パケットの DSCP 値を生成します。

trust dscp を指定した場合、QoS は入力パケットから DSCP 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値、タグなしの非 IP パケットに対しては、デフォルトポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

trust ip-precedence を指定した場合、QoS は入力パケットおよび IP precedence/DSCP マップから IP precedence 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値、タグなしの非 IP パケットに対しては、デフォルトポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

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。

例

次の例では、*class1* で分類されたトラフィックの着信 DSCP 値を信頼するため、ポート信頼状態を定義する方法を示します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# 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。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件 (police 、 set 、および trust ポリシーマップ クラス コンフィギュレーション コマンドによる) を定義します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー マップを作成または変更します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	QoS ポリシー マップを表示します。

udld

単方向リンク検出 (UDLD) でアグレッシブ モードまたはノーマル モードをイネーブルにし、設定可能なメッセージ タイマー時間を設定するには、**udld** 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。すべての光ファイバポートでアグレッシブ モードまたはノーマル モードの 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}
```

シンタックスの説明

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、ノーマル 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 フェーズにあり、双方向と判別されたポートにおける UDLD プローブ 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 7 ~ 90 秒です。

デフォルト

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 60 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

UDLD は、ノーマル モード (デフォルト) とアグレッシブ モードという 2 つの動作モードをサポートしています。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。ノーマル モードとアグレッシブ モードの詳細については、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 ガイドの「Understanding UDLD」を参照してください。

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 負荷のトレードオフを行っていることとなります。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。

UDLD によるインターフェイス シャットダウンをリセットするのに、以下のコマンドを使用できます。

- **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 コマンド
- **no udld enable** グローバル コンフィギュレーション コマンドのあとに **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 コマンドのあとに **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 - 指定されたインターフェイスの 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 errdisable ステートから回復します。

例

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。

```
Switch(config)# udld enable
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show udld	すべてのポートまたは指定されたポートの UDLD 管理上および運用上のステータスを表示します。
udld port	個々のインターフェイスで 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 udld グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。
udld reset	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、トラフィックが再び通過するのを許可します。

udld port

個々のインターフェイス上で 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 **udld** グローバル コンフィギュレーション コマンドでイネーブルにならないようにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。**udld** グローバル コンフィギュレーション コマンド設定に戻したり、非光ファイバポートで入力された場合に UDLD をディセーブルしたりする場合は、このコマンドの **no** 形式を使用します。

udld port [aggressive]

no udld port [aggressive]

シンタックスの説明

aggressive	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。
-------------------	--

デフォルト

光ファイバインターフェイスでは、UDLD はイネーブル、アグレッシブ モード、ディセーブルのいずれでもありません。このため、光ファイバインターフェイスは、**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドのステートに従い 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。

コマンドモード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合は、このポートは単一方向リンクを検出できません。

UDLD は、ノーマル モード（デフォルト）とアグレッシブ モードという 2 つの動作モードをサポートしています。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。ノーマル モードとアグレッシブ モードの詳細については、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 ガイドの「Configuring UDLD」の章を参照してください。

UDLD をノーマル モードでイネーブルにするには、**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、**udld port aggressive** インターフェイス コンフィギュレーション コマンドを使用します。

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。

udld enable または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を無効にする場合は、光ファイバポートで **udld port aggressive** コマンドを使用します。設定を削除して UDLD イネーブル化の制御を **udld** 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** 形式を使用します。

UDLD によるインターフェイス シャットダウンをリセットするのに、以下のコマンドを使用できます。

- **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 コマンド
- **no udld enable** グローバル コンフィギュレーション コマンドのあとに **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 コマンドのあとに **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 - 指定されたインターフェイスの 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 errdisable ステートから回復します。

例 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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

次の例では、**udld** グローバル コンフィギュレーション 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。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

設定を確認するには、**show running-config** または **show udld interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
show udld	すべてのポートまたは指定されたポートの UDLD 管理上および運用上のステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
udld reset	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、トラフィックが再び通過するのを許可します。

udld reset

単一方向リンク検出 (UDLD) によってディセーブルになったインターフェイスをすべてリセットし、トラフィックの転送を再び許可するには、**udld reset** 特権 EXEC 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]、Dynamic Trunking Protocol [DTP] などの他の機能が有効になります)。

udld reset

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 の稼動を開始し、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。

例

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。

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
show udld	すべてのポートまたは指定されたポートの UDLD 管理上および運用上のステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
udld port	個々のインターフェイスで 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 udld グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。

vlan (グローバル コンフィギュレーション)

VLAN を追加して `config-vlan` モードを開始するには、`vlan` 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。VLAN を削除する場合は、このコマンドの `no` 形式を使用します。標準範囲 VLAN (VLAN ID 1 ~ 1005) のコンフィギュレーション情報は、常に VLAN データベースに保存されます。VLAN トランッキング プロトコル (VTP) モードが透過の場合は、拡張範囲 VLAN (VLAN ID が 1006 以上) を作成できます。これにより、VTP モード、ドメイン名、および VLAN 設定がスイッチ実行コンフィギュレーション ファイルに保存されます。`copy running-config startup-config` 特権 EXEC コマンドを使用すれば、設定をスイッチ 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。

```
vlan vlan-id
```

```
no vlan vlan-id
```

シンタックスの説明

<i>vlan-id</i>	追加および設定する VLAN の ID。 <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。VLAN ID を単独で入力したり、それぞれをカンマで区切って一連の VLAN ID を入力したり、ハイフンを間に挿入して VLAN ID の範囲を入力したりすることができます。
----------------	---

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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 コマンドを使用する必要があります。拡張範囲で VLAN を設定する前に、`vtp transparent` グローバル コンフィギュレーション コマンドまたは `VLAN` コンフィギュレーション コマンドを使用してスイッチを VTP 透過モードにします。拡張範囲 VLAN は、VTP によって学習されず、VLAN データベースにも追加されませんが、VTP モードが透過型である場合には、VTP モード、ドメイン名、およびすべての VLAN 設定は、実行コンフィギュレーションに保存され、これをスイッチ 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こともできます。

VLAN 設定と 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スイッチを再起動すると、設定が次のように選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードが透過型であり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。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。
- VTP モードがサーバの場合、またはスタートアップ 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、最初の 1005 個の VLAN の VTP モードおよび VLAN 設定には VLAN データベース情報が使用されます。

スイッチが VTP 透過モードでない場合に拡張範囲 VLAN を作成しようとする、VLAN は拒否され、エラー メッセージが表示されます。

無効な VLAN ID を入力すると、エラー メッセージが表示され、`config-vlan` モードを開始できません。

`vlan` コマンドを VLAN ID とともに入力すると、`config-vlan` 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、`config-vlan` 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。

次のコンフィギュレーション コマンドが `config-vlan` モードで利用できます。このコマンドの `no` 形式を使用すると、特性がそのデフォルト ステートに戻ります。



(注)

すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされている VLAN コンフィギュレーション コマンドは `mtu mtu-size` と `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 ステートのままにしておく必要があります。

- **are are-number** : この VLAN の All-Route Explorer (ARE) ホップの最大数を定義します。このキーワードは、TrCRF VLAN にだけ適用されます。指定できる範囲は 0 ~ 13 です。デフォルト値は 7 です。値が入力されていない場合は、0 が最大数と見なされます。
- **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。
 - この VLAN のバックアップ CRF モードを **enable** (イネーブル) にします。
 - この VLAN のバックアップ CRF モードを **disable** (ディセーブル) にします (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 内でこの VLAN が親 VLAN として設定されている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 のデフォルトブリッジ番号は 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 にだけ適用され、次のうちの 1 つです。
 - **srb** (Source-Route Bridge [SRB; ソースルートブリッジ])
 - **srt** (ソースルートトランスペアレント [SRT]) 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 のみ) を増分して、`config-vlan` モードを終了します。
- **media** : VLAN メディア タイプを定義します。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、表 2-41 を参照してください。



(注)

スイッチ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、別のスイッチに対する VLAN トランッキングプロトコル (VTP) グローバルアドバタイズにかぎって設定します。これらの VLAN はローカルに停止されます。

- **ethernet** は、イーサネットメディアタイプです (デフォルト)。
- **fddi** は、FDDI メディアタイプです。
- **fd-net** は、FDDI-NET メディアタイプです。
- **tokenring** は、VTP v2 モードがディセーブルの場合にはトークンリングメディアタイプであり、VTP v2 モードがイネーブルの場合は TrCRF です。

- **tr-net** は、VTP v2 モードがディセーブルの場合にはトークンリング NET メディア タイプであり、VTP v2 モードがイネーブルの場合は TrBRF メディア タイプです。
- **mtu mtu-size** : MTU を指定します (バイト単位のパケット サイズ)。指定できる範囲は 1500 ~ 18190 です。デフォルト値は 1500 バイトです。
- **name vlan-name** : 管理ドメイン内で一意にする必要のある VLAN 名を 1 ~ 32 文字の ASCII 文字列で指定します。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、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 を定義するときには必要です。指定できる範囲は 0 ~ 1005 です。FDDI およびトークンリング VLAN のデフォルトの親 VLAN ID は 0 (親 VLAN なし) です。トークンリングおよび TrCRF VLAN では、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化されます。VTP がイネーブルの場合、新しい RSPAN VLAN は、VLAN ID が 1024 より小さい VLAN 用の VTP で伝播されます。ラーニングは VLAN 上でディセーブルになります。詳細については、**remote-span** コマンドを参照してください。
- **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、デフォルト値がありません。
- **said said-value** : IEEE 802.10 に記載されている Security Association Identifier (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wit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、**config-vlan** モードを終了したときに有効になります。
- **state** : VLAN ステートを指定します。
 - **active** は、VLAN が稼動中であることを意味します (デフォルト)。
 - **suspend** は、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** : Spanning-Tree Explorer (STE; スパニングツリー エクスプローラ) 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、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。
 - SRTブリッジングを実行している IEEE イーサネット STP の場合は、**ieee**
 - SRB を実行している IBM STP の場合は、**ibm**
 - SRTブリッジング (IEEE) および SRB (IBM) の組み合わせを実行している STP の場合は、**auto**

- **tb-vlan1** *tb-vlan1-id* および **tb-vlan2** *tb-vlan2-id* : この VLAN とのトランスレーショナルブリッジングが最初に行われる VLAN と 2 番目に実行される 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。値が指定されていない場合は、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。

表 2-41 さまざまなメディア タイプに有効なコマンドと構文

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> 、 mtu <i>mtu-size</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> 、 mtu <i>mtu-size</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>
FDDI-NET	name <i>vlan-name</i> 、 media fd-net 、 state {suspend active}、 said <i>said-value</i> 、 mtu <i>mtu-size</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> VTP v2 モードがディセーブルの場合、 stp type を auto に設定しないでください。
トークンリング	VTP v1 モードはイネーブルです。 name <i>vlan-name</i> 、 media tokenring 、 state {suspend active}、 said <i>said-value</i> 、 mtu <i>mtu-size</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>
TrCRF	VTP v2 モードはイネーブルです。 name <i>vlan-name</i> 、 media tokenring 、 state {suspend active}、 said <i>said-value</i> 、 mtu <i>mtu-size</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>
トークンリング NET	VTP v1 モードはイネーブルです。 name <i>vlan-name</i> 、 media tr-net 、 state {suspend active}、 said <i>said-value</i> 、 mtu <i>mtu-size</i> 、 bridge <i>bridge-number</i> 、 stp type {ieee ibm}、 tb-vlan1 <i>tb-vlan1-id</i> 、 tb-vlan2 <i>tb-vlan2-id</i>
TrBRF	VTP v2 モードはイネーブルです。 name <i>vlan-name</i> 、 media tr-net 、 state {suspend active}、 said <i>said-value</i> 、 mtu <i>mtu-size</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>

表 2-42 に、VLAN の設定規則を示します。

表 2-42 VLAN 設定規則

設定	規則
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	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。 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。 各 TrCRF VLAN の親 VLAN ID が同じ場合に一意のリング番号を指定します。1 つのバックアップ Concentrator Relay Function (CRF; コンセントレータ リレー機能) だけをイネーブルにすることができます。
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	VLAN の STP タイプを auto に設定しないでください。 この規則は、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。
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)	使用されるトランスレーショナルブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 (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 へのポイントが含まれている必要があります。 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 VLAN ID 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 とは異なったメディア タイプである必要があります。 両方のトランスレーショナルブリッジング VLAN ID 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 は異なったメディア タイプである必要があります。

例

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 `VLANxxx` 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` オプションは **ethernet** です。 `state` オプションは **active** です。デフォルトの `said-value` 変数は、100000 に VLAN ID を加算した値です。 `mtu-size` 変数は 1500、 `stp-type` オプションは **ieee** です。 `exit config-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しません。

次の例では、新しい VLAN をすべてデフォルト特性で作成し、`config-vlan` モードを開始する方法を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

次の例では、すべての特性がデフォルトである拡張範囲 VLAN を新規作成し、`config-vlan` モードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する方法を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# 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。

関連コマンド

コマンド	説明
show vlan	すべての設定された VLAN または 1 つの VLAN (VLAN ID または名前が指定されている場合) のパラメータを管理ドメインに表示します。
vlan (VLAN コンフィギュレーション)	標準範囲 VLAN を VLAN データベースに設定します。

vlan (VLAN コンフィギュレーション)

VLAN データベースに標準範囲 VLAN (VLAN ID 1 ~ 1005) の VLAN 特性を設定するには、**vlan** VLAN コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** 特権 EXEC コマンドを入力します。VLAN を削除する場合は、追加パラメータなしでこのコマンドの **no** 形式を使用します。設定された特性を変更する場合は、パラメータとともにこのコマンドの **no** 形式を使用します。

```
vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number |
type {srb | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

```
no vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number |
type {srb | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

拡張範囲 VLAN (VLAN ID 1006 ~ 4094) は、これらのコマンドを使用して追加することも変更することもできません。拡張範囲 VLAN を追加する場合は、**vlan (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 **config-vlan** モードを開始します。



(注)

スイッチ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、別のスイッチに対する VLAN トランッキング プロトコル (VTP) グローバル アドバタイズにかぎって設定します。これらの VLAN はローカルに停止されます。

シンタックスの説明

<i>vlan-id</i>	設定された VLAN の ID。指定できる ID は、1 ~ 1005 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。先行ゼロは入力しないでください。
are are-number	(任意) この VLAN の All-Route Explorer (ARE) ホップの最大数を指定します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ~ 13 です。値が入力されていない場合は、0 が最大数と見なされます。
backupcrf {enable disable}	(任意) バックアップ コンセントレータ リレー機能 (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。 <ul style="list-style-type: none"> この VLAN のバックアップ CRF モードを enable (イネーブル) にします。 この VLAN のバックアップ CRF モードを disable (ディセーブル) にします。

bridge <i>bridge-number</i> type { srb srt }	(任意) 論理分散ソース ルーティング ブリッジ、つまり FDDI-Network Entity Title (NET)、トークンリング NET、および Token Ring Bridge Relay Function (TrBRF; トークンリング ブリッジ リレー機能) 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。 type キーワードは、TrCRF VLAN にだけ適用され、次のうちの 1 つです。 <ul style="list-style-type: none"> • srb (ソースルートブリッジ [SRB]) • srt (ソースルート トランスペアレント [SRT]) ブリッジング VLAN
media { ethernet fddi fd-net tokenring tr-net }	(任意) VLAN メディア タイプを指定します。表 2-43 に、各メディア タイプに有効な構文を示します。 <ul style="list-style-type: none"> • ethernet は、イーサネット メディア タイプです (デフォルト)。 • fddi は、FDDI メディア タイプです。 • fd-net は、FDDI-NET メディア タイプです。 • tokenring は、VTP v2 モードがディセーブルの場合にはトークンリング メディア タイプであり、VTP v2 モードがイネーブルの場合は TrCRF です。 • tr-net は、VTP v2 モードがディセーブルの場合にはトークンリング NET メディア タイプであり、VTP v2 モードがイネーブルの場合は TrBRF メディア タイプです。
mtu <i>mtu-size</i>	(任意) 最大伝送ユニット (MTU) (バイト単位の packetsize) を指定します。指定できる範囲は 1500 ~ 18190 です。
name <i>vlan-name</i>	(任意) 管理ドメイン内で一意である 1 ~ 32 文字の ASCII 文字列で VLAN 名を指定します。
parent <i>parent-vlan-id</i>	(任意) 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 を定義するときに必要です。指定できる範囲は 0 ~ 1005 です。
ring <i>ring-number</i>	(任意) 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。
said <i>said-value</i>	(任意) IEEE 802.10 に記載されている Security Association Identifier (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。
state { suspend active }	(任意) VLAN ステートを指定します。 <ul style="list-style-type: none"> • active である場合、VLAN は稼働中です。 • suspend の場合、VLAN は停止しています。停止している VLAN はパケットを通過させません。
ste <i>ste-number</i>	(任意) STE (スパニングツリー エクスプローラ) ホップの最大数を指定します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ~ 13 です。

stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }	(任意) FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニングツリー タイプを指定します。 <ul style="list-style-type: none"> • SRTブリッジングを実行している IEEE イーサネット STP の場合は、ieee • SRB を実行している IBM STP の場合は、ibm • SRTブリッジング (IEEE) および SRB (IBM) の組み合わせを実行している STP の場合は、auto
tb-vlan1 <i>tb-vlan1-id</i> および tb-vlan2 <i>tb-vlan2-id</i>	(任意) 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。値が指定されていない場合は、0 と見なされます。

表 2-43 に、さまざまなメディア タイプで指定できる構文オプションを示します。

表 2-43 さまざまなメディア タイプに有効な構文

メディア タイプ	指定できる構文
イーサネット	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media ethernet [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
FDDI	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fddi [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</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>]
FDDI-NET	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fd-net [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] VTP v2 モードがディセーブルの場合、 stp type を auto に設定しないでください。
トークンリング	VTP v1 モードはイネーブルです。 vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</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>]
TrCRF	VTP v2 モードはイネーブルです。 vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [bridge type { <i>srb</i> <i>srt</i> }] [are <i>are-number</i>] [ste <i>ste-number</i>] [backupcrf { <i>enable</i> <i>disable</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
トークンリング NET	VTP v1 モードはイネーブルです。 vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { <i>ieee</i> <i>ibm</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
TrBRF	VTP v2 モードはイネーブルです。 vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { <i>suspend</i> <i>active</i> }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]

表 2-44 に、VLAN の設定規則を示します。

表 2-44 VLAN 設定規則

設定	規則
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	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。 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。 各 TrCRF VLAN の親 VLAN ID が同じ場合に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。
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	VLAN の STP タイプを auto に設定しないでください。 この規則は、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。
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)	使用されるトランスレーショナルブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 (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 へのポイントが含まれている必要があります。 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 VLAN ID 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 とは異なったメディアタイプである必要があります。 両方のトランスレーショナルブリッジング VLAN ID 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 は異なったメディアタイプである必要があります。

デフォルト

ARE 値は 7 です。

バックアップ CRF はディセーブルです。

FDDI-NET、TrBRF、およびトークンリング NET VLAN については、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。

media タイプは **ethernet** です。

デフォルトの *mtu size* は 1500 バイトです。

vlan-name 変数は *VLANxxx* です。ここで、*xxx* は VLAN ID 番号と同じ 4 桁の数字 (先行ゼロを含む) です。

■ vlan (VLAN コンフィギュレーション)

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。TrCRF VLAN では、親 VLAN ID を指定する必要があります。トークンリングおよび TrCRF VLAN では、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。

トークンリング VLAN の *ring number* は 0 です。FDDI VLAN には、デフォルト値がありません。

said value は、100000 に VLAN ID 番号を加算した値です。

ステータスは **active** です。

STE 値は 7 です。

STP タイプは、FDDI-NET では **ieee**、トークンリング NET VLAN では **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。

tb-vlan1-id および *tb-vlan2-id* 変数は 0 (トランスレーショナルブリッジングなし) です。

コマンドモード

VLAN コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドモードを使用できるのは、標準範囲 VLAN (VLAN ID 1 ~ 1005) を設定する場合だけです。



(注)

拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を設定する場合は、**vlan** 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ください。

VTP の設定は常に VLAN データベースに保存されます。VTP モードが透過型の場合、VTP 設定は、VTP モードおよびドメイン名とともにスイッチの実行コンフィギュレーション ファイルにも保存されます。**copy running-config startup-config** 特権 EXEC コマンドを使用すれば、これをスイッチ 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。

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スイッチを再起動した場合、設定は次のように選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードが透過型であり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。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。
- VTP モードがサーバである場合、またはスタートアップ 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、最初の 1005 の VLAN の 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。

no vlan コマンドを使用した結果は次のとおりです。

- **no vlan vlan-id** 形式を使用すると、VLAN は削除されます。VLAN を削除すると、削除された VLAN を参照する他の親 VLAN およびトランスレーショナルブリッジングパラメータは自動的に 0 にリセットされます。
- **no vlan vlan-id bridge** 形式を使用すると、VLAN ソースルーティングブリッジ番号はデフォルトの 0 に戻ります。**vlan vlan-id bridge** コマンドは、FDDI-NET およびトークンリング NET VLAN でのみ使用され、他の VLAN タイプでは無視されます。
- **no vlan vlan-id media** 形式を使用すると、メディアタイプはデフォルト (**ethernet**) に戻ります。VLAN メディアタイプ (**no** 形式を含む) を変更すると、(そのコマンドに **mtu** キーワードも存在しない場合) VLAN MTU はそのタイプのデフォルトの MTU にリセットされます。また、VLAN の親 VLAN およびトランスレーショナルブリッジング VLAN も (そのコマンドに **parent**、**tb-vlan1** または **tb-vlan2** も存在しない場合) デフォルトにリセットされます。
- **no vlan vlan-id mtu** 形式を使用すると、VLAN MTU は適用可能な VLAN メディアタイプのデフォルトに戻ります。**media** キーワードを使用しても MTU を変更できます。
- **no vlan vlan-id name vlan-name** 形式を使用すると、VLAN 名はデフォルト名に戻ります (**VLANxxxx**、ここで **xxxx** は VLAN ID 番号に等しい 4 桁の数字 [先行ゼロを含む] です)。
- **no vlan vlan-id parent** 形式を使用すると、親 VLAN はデフォルト (0) に戻ります。親 VLAN が削除された場合、または **media** キーワードによって VLAN タイプまたは親 VLAN の VLAN タイプが変更された場合、親 VLAN はデフォルトにリセットされます。
- **no vlan vlan-id ring** 形式を使用すると、VLAN 論理リング番号はデフォルト (0) に戻ります。
- **no vlan vlan-id said** 形式を使用すると、VLAN SAID はデフォルト (100000 に VLAN ID を加算した値) に戻ります。
- **no vlan vlan-id state** 形式を使用すると、VLAN ステータスはデフォルト (**active**) に戻ります。
- **no vlan vlan-id stp type** 形式を使用すると、VLAN スパニングツリータイプはデフォルト (**ieee**) に戻ります。
- **no vlan vlan-id tb-vlan1** または **no -id tb-vlan2** 形式を使用すると、1 つまたは複数の VLAN トランスレーショナルブリッジ VLAN はデフォルト (0) に戻ります。トランスレーショナルブリッジ VLAN は、影響を受ける VLAN とは異なった VLAN タイプである必要があります。2 つ指定した場合には、この 2 つが互いに異なった VLAN タイプである必要があります。トランスレーショナルブリッジ VLAN が削除された場合、**media** キーワードにより VLAN タイプが変更された場合、または **media** キーワードにより対応するトランスレーショナルブリッジ VLAN の VLAN タイプが変更された場合、トランスレーショナルブリッジ VLAN はデフォルトに戻ります。

例

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 **VLANxxx** 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** オプションは **ethernet** です。**state** オプションは **active** です。デフォルトの **said-value** 変数は、100000 に VLAN ID を加算した値です。**mtu-size** 変数は 1500、**stp-type** オプションは **ieee** です。**exit** または **apply 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。

```
Switch(vlan)# vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)# exit
APPLY completed.
Exiting....
```

■ vlan (VLAN コンフィギュレーション)

次の例では、名前および MTU サイズを変更することにより既存の VLAN を変更する方法を示します。

```
Switch(vlan)# no vlan name engineering mtu 1200
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vlan	すべての設定された VLAN または 1 つの VLAN (VLAN ID または名前が指定されている場合) のパラメータを管理ドメインに表示します。
vlan (グローバル コンフィギュレーション)	標準範囲および拡張範囲 VLAN を設定するための config-vlan モードを開始します。

vlan database

VLAN コンフィギュレーション モードを開始するには、**vlan database** 特権 EXEC コマンドを入力します。このモードから、標準範囲 VLAN の VLAN 設定の追加、削除、および変更を行い、VLAN トランッキング プロトコル (VTP) を使用してこれらの変更をグローバルに伝播できます。コンフィギュレーション情報は、VLAN データベースに保存されます。

vlan database



(注) VLAN コンフィギュレーション モードは、VLAN ID が 1 ~ 1005 の VLAN にのみ有効となります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VLAN データベース コンフィギュレーション コマンドを使用すると、VLAN 1 ~ 1005 を設定できます。拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を設定するには、**vlan (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 **config-vlan** モードを開始します。また、**vlan** 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 VLAN ID 1 ~ 1005 を設定することもできます。

VLAN 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。



(注) このコマンド モードはセッション指向であるため、他のモードとは異なっています。VLAN パラメータを追加、削除、または変更した場合、**apply** または **exit** コマンドを入力してセッションを終了するまでその変更は適用されません。変更が適用されると、VTP コンフィギュレーション バージョンは増分されます。**abort** を入力して変更を VTP データベースに適用しないこともできます。

VLAN コンフィギュレーション モードに入っている場合は、VLAN データベースにアクセスし、次のコマンドを使用して変更を加えることができます。

- **vlan** : サブコマンドにアクセスして、1 つの VLAN に関連付けられた値を追加、削除、または変更します。詳細については、**vlan (VLAN コンフィギュレーション)** コマンドを参照してください。
- **vtp** : サブコマンドにアクセスして、VTP 管理機能を実行します。詳細については、**vtp (VLAN コンフィギュレーション)** コマンドを参照してください。

VLAN または VTP パラメータを変更した場合、次の編集バッファ処理コマンドを使用できます。

- **abort** : 変更を適用せずにこのモードを終了します。VLAN コンフィギュレーション モードを開始する前に稼動していた VLAN 設定を引き続き使用します。
- **apply** : 現在の変更を VLAN データベースに適用し、データベース コンフィギュレーション リビジョン番号を増分し、管理ドメイン全体にこれを伝播し、VLAN コンフィギュレーション モードを継続します。



(注) スイッチが VTP クライアント モードである場合にはこのコマンドを使用することはできません。

- **exit** : すべてのコンフィギュレーション変更を VLAN データベースに適用し、データベース コンフィギュレーション番号を増分し、管理ドメイン全体にこれを伝播し、特権 EXEC モードに戻ります。
- **no** : コマンドを無効にするか、デフォルトに設定します。指定できる値は **vlan** および **vtp** です。
- **reset** : VLAN データベースに加える予定の変更を破棄し、設定する予定のデータベースをスイッチ上で実施されている VLAN データベースにリセットし、VLAN コンフィギュレーション モードを継続します。
- **show** : VLAN データベース情報を表示します。
- **show changes [vlan-id]** : すべての標準範囲 VLAN ID (1 ~ 1005) または指定された VLAN ID (1 ~ 1005) に関して、スイッチ上の VLAN データベースと設定する予定の VLAN データベース間の相違を表示します。
- **show current [vlan-id]** : スイッチ上または選択された VLAN (1 ~ 1005) 上の VLAN データベースを表示します。
- **show proposed [vlan-id]** : 設定する予定の VLAN データベースを表示するか、または設定する予定のデータベースから選択した VLAN (1 ~ 1005) を表示します。設定しようとしている VLAN データベースは、**exit** または **apply** VLAN コンフィギュレーション コマンドを使用するまで実行コンフィギュレーションではありません。

show vlan 特権 EXEC コマンドを入力すると、VLAN データベース変更が行われたのか、それとも打ち切られたのかを確認できます。出力は、**show** VLAN データベース コンフィギュレーション コマンドの出力とは異なります。

例

次の例では、特権 EXEC コマンドモードから VLAN コンフィギュレーション モードを開始して、VLAN データベース情報を表示する方法を示します。

```
Switch# vlan database
Switch(vlan)# show
VLAN ISL Id: 1
  Name: default
  Media Type: Ethernet
  VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003

VLAN ISL Id: 2
  Name: VLAN0002
  Media Type: Ethernet
  VLAN 802.10 Id: 100002
  State: Operational
```

```

MTU: 1500

VLAN ISL Id: 1002
Name: fddi-default
Media Type: FDDI
VLAN 802.10 Id: 101002
State: Operational
MTU: 1500
Bridge Type: SRB
Ring Number: 0
Translational Bridged VLAN: 1
Translational Bridged VLAN: 1003

```

<output truncated>

次の例では、**show changes** コマンドの出力を示します。

```
Switch(vlan)# show changes
```

```

DELETED:
VLAN ISL Id: 4
Name: VLAN0004
Media Type: Ethernet
VLAN 802.10 Id: 100004
State: Operational
MTU: 1500

```

```

MODIFIED:
VLAN ISL Id: 7
Current State: Operational
Modified State: Suspended

```

次の例では、現在のデータベースの VLAN 7 と設定しようとしているデータベースとの相違を表示する方法を示します。

```
Switch(vlan)# show changes 7
```

```

MODIFIED:
VLAN ISL Id: 7
Current State: Operational
Modified State: Suspended

```

次の例では、**show current 20** コマンドの出力を示します。現在のデータベースの VLAN 20 だけが表示されます。

```

Switch(vlan)# show current 20
VLAN ISL Id: 20
Name: VLAN0020
Media Type: Ethernet
VLAN 802.10 Id: 100020
State: Operational
MTU: 1500

```

関連コマンド

コマンド	説明
show vlan	管理ドメイン内のすべての設定された VLAN のパラメータを表示します。
shutdown vlan	指定された VLAN でローカルトラフィックをシャットダウン (停止) します。
vlan (グローバルコンフィギュレーション)	標準範囲および拡張範囲 VLAN を設定するための config-vlan モードを開始します。

vmps reconfirm (特権 EXEC)

ただちに VQP クエリーを送信して VMPS でのすべてのダイナミック VLAN 割り当てを再確認するには、**vmps reconfirm** 特権 EXEC コマンドを使用します。

vmps reconfirm

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、VQP クエリーを VMPS にただちに送信する方法を示します。

```
Switch# vmps reconfirm
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Reconfirmation Status セクションの VMPS Action 列を調べます。**show vmps** コマンドは、再確認タイマー切れの結果または **vmps reconfirm** コマンドの入力のいずれかにより最後に割り当てが再確認された結果を表示します。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。
vmps reconfirm (グローバル コンフィギュレーション)	VQP クライアントの再確認間隔を変更します。

vmps reconfirm (グローバル コンフィギュレーション)

VLAN Query Protocol (VQP) クライアントの再確認の間隔を変更するには、**vmps reconfirm** 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。

vmps reconfirm *interval*

no vmps reconfirm

シンタックスの説明	<i>interval</i>	ダイナミック VLAN 割り当てを再確認するための VLAN メンバシップ ポリシー サーバ (VMPS) への VQP クライアント クエリーの再確認間隔。指定できる範囲は 1 ~ 120 分です。
-----------	-----------------	--

デフォルト デフォルトの再確認間隔は 60 分です。

コマンド モード グローバル コンフィギュレーション

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

例 次の例では、VQP クライアントが 20 分ごとにダイナミック VLAN エントリを再確認するように設定する方法を示します。

```
Switch(config)# vmps reconfirm 20
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Reconfirm Interval 列を調べます。

関連コマンド	コマンド	説明
	show vmps	VQP および VMPS 情報を表示します。
	vmps reconfirm (特権 EXEC)	VQP クエリーを送信して、VMPS でのすべてのダイナミック VLAN 割り当てを再確認します。

vmps retry

VLAN Query Protocol (VQP) クライアントに関してサーバごとの再試行回数を設定するには、**vmps retry** 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。

vmps retry count

no vmps retry

シンタックスの説明

<i>count</i>	リストの次のサーバに照会する前にクライアントが VLAN メンバシップ ポリシーサーバ (VMPS) との通信を試行する回数。指定できる範囲は 1 ~ 10 です。
--------------	--

デフォルト

デフォルトの再試行回数は 3 です。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、再試行回数を 7 に設定する方法を示します。

```
Switch(config)# vmps retry 7
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Server Retry Count 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。

vmps server

プライマリ VMPS と 3 つまでのセカンダリ サーバを設定するには、**vmps server** 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。VMPS 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。

vmps server *ipaddress* [primary]

no vmps server [*ipaddress*]

シンタックスの説明

<i>ipaddress</i>	プライマリまたはセカンダリ VMPS サーバの IP アドレスまたはホスト名。ホスト名を指定する場合には、Domain Name System (DNS; ドメイン ネーム システム) サーバが設定されている必要があります。
primary	(任意) プライマリとセカンダリのどちらの VMPS サーバを設定するのかを決定します。

デフォルト

プライマリまたはセカンダリ VMPS サーバは定義されていません。

コマンドモード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

primary が入力されているかどうかにかかわらず、最初に入力されたサーバは自動的にプライマリサーバとして選択されます。最初のサーバアドレスは、次のコマンドで **primary** を使用することにより無効にすることができます。

クラスタ コンフィギュレーションのメンバー スイッチに IP アドレスがない場合、クラスタはそのメンバー スイッチに設定された VMPS サーバを使用しません。その代わりに、クラスタはコマンド スイッチの VMPS サーバを使用し、コマンド スイッチは VMPS 要求のプロキシとなります。VMPS サーバは、クラスタを単一スイッチとして扱い、コマンド スイッチの IP アドレスを使用して要求に応答します。

ipaddress を指定せずに **no** 形式を使用すると、すべての設定されたサーバが削除されます。ダイナミック アクセス ポートが存在するときにすべてのサーバを削除すると、スイッチは、VMPS に照会できないため、これらのポートの新しい送信元からのパケットを転送できません。

例

次の例では、IP アドレス 191.10.49.20 をプライマリ VMPS サーバとして設定する方法を示します。IP アドレス 191.10.49.21 および 191.10.49.22 のサーバは、セカンダリ サーバとして設定されます。

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

次の例では、IP アドレス 191.10.49.21 のサーバを削除する方法を示します。

```
Switch(config)# no vmps server 191.10.49.21
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、VMPS Domain Server 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。

vtp (グローバル コンフィギュレーション)

VTP 設定の特性を設定または修正するには、**vtp** 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。設定を削除したり、デフォルト設定に戻したりする場合は、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** {**client** | **server** | **transparent**} | **password** *password* | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** | **password** | **pruning** | **version**}

シンタックスの説明	
domain <i>domain-name</i>	VTP ドメイン名をスイッチの 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せん。
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>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 アドレスのみ使用します。
mode	VTP 装置モードをクライアント、サーバ、または透過型に指定します。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信できますが、VLAN 設定を保存する十分な不揮発性メモリを持ちません。スイッチで VLAN を設定することはできません。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。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信します。スイッチで VLAN を設定できます。スイッチは、再起動後不揮発性メモリから現在の VTP データベースのすべての VLAN 情報を回復できます。
transparent	スイッチを VTP 透過モードにします。VTP 透過モードのスイッチは VTP がディセーブルになっており、アドバタイズを送信したり、他の装置が送信したアドバタイズから学習したりしません。また、ネットワーク内の他の装置の VLAN 設定に影響を与えることはできません。スイッチは VTP アドバタイズを受信し、アドバタイズ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。 VTP モードが透過型である場合、モードおよびドメイン名は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。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、 copy running-config startup-config 特権 EXEC コマンドを入力します。
password <i>password</i>	VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための 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。
pruning	スイッチ上で VTP プルーニングをイネーブルに設定します。
version <i>number</i>	VTP バージョンをバージョン 1 またはバージョン 2 に設定します。

デフォルト

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。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VTP モード、VTP ドメイン名、および VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードが透過型であり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。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 VTP モードがサーバ モードの場合、またはスタートアップ 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、最初の 1005 の VTP および VLAN 設定は、VLAN データベース情報によって選択され、1005 を超える VLAN は、スイッチ コンフィギュレーション ファイルから設定されます。

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、スイッチは非管理ドメイン ステートに置かれます。非管理ドメイン ステートに置かれている間は、ローカル VLAN 設定に変更が生じてもスイッチは VTP アドバタイズを送信しません。スイッチは、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あと、または **vtp domain** コマンドでドメイン名を設定したあとで、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信すると、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから出たあと、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もう一度入るように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ことができるわけではありません。

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、スイッチを 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、スイッチがクライアント モードまたはトランスパレント モードでない場合にエラーを戻さないことを除けば、**no vtp mode** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバのコンフィギュレーションをコピーします。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたは透過モードである場合、スイッチの設定は変更されません。
- 透過モードのスイッチは、VTP に参加しません。透過モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードにあるスイッチで 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スイッチに伝播されます。
- **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、スイッチからドメインを削除しません。
- 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 モードは透過型に設定してください。
- 拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、そのコンフィギュレーションは許可されません。
- 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かぎります。

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。

- パスワードでは、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スイッチで一致している必要があります。
- スイッチ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。

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 サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ~ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、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 ステートのトグリングを行うと、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 スイッチは他のすべての 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 スイッチでバージョン 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 モードで稼動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スイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 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 対応スイッチに伝播されます。
- 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。

vtp (グローバル コンフィギュレーション)

- トークンリングブリッジリレー機能 (TrBRF) または Token Ring Concentrator Relay Function (TrCRF; トークンリング コンセントレータ リレー機能) VLAN メディア タイプを設定している場合は、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 NET VLAN 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。

スイッチ コンフィギュレーション ファイルにパスワード、プルーニング、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。

例

次の例では、VTP コンフィギュレーション メモリのファイル名を *vtpfilename* に変更する方法を示します。

```
Switch(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。

```
Switch(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。

```
Switch(config)# vtp interface gigabitethernet
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(config)# vtp domain OurDomainName
```

次の例では、スイッチを VTP 透過モードにする方法を示します。

```
Switch(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。

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

次の例では、VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Switch(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。

```
Switch(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。

関連コマンド

コマンド	説明
show vtp status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
vtp (VLAN コンフィギュレーション)	VTP のドメイン名、パスワード、プルーニング、バージョンおよびモードを設定します。

vtp (VLAN コンフィギュレーション)

VTP の特性を設定するには、**vtp** VLAN コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** 特権 EXEC コマンドを入力します。デフォルト設定に戻したり、特性をディセーブルにしたり、パスワードを削除したりする場合は、このコマンドの **no** 形式を使用します。

```
vtp {domain domain-name | password password | pruning | v2-mode | {server | client | transparent}}
```

```
no vtp {client | password | pruning | transparent | v2-mode}
```

シンタックスの説明

domain <i>domain-name</i>	スイッチの VTP 管理ドメインを識別する VTP ドメイン名を、1 ～ 32 文字の ASCII 文字列を入力して設定します。ドメイン名では大文字と小文字が区別されます。
password <i>password</i>	VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための 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。
pruning	VTP 管理ドメインでプルーンングをイネーブルにします。VTP プルーンングは、プルーンング適格 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。
v2-mode	管理ドメインで VLAN トランキング プロトコル (VTP) バージョン 2 をイネーブルにします。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信できますが、VLAN 設定を保存する十分な不揮発性メモリを持ちません。スイッチで VLAN を設定することはできません。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。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信します。スイッチで VLAN を設定できます。スイッチは、再起動後不揮発性メモリから現在の VTP データベースのすべての VLAN 情報を回復できます。
transparent	スイッチを VTP 透過モードにします。VTP 透過モードのスイッチは VTP がディセーブルになっており、アドバタイズを送信したり、他の装置が送信したアドバタイズから学習したりしません。また、ネットワーク内の他の装置の VLAN 設定に影響を与えることはできません。スイッチは VTP アドバタイズを受信し、アドバタイズ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。

デフォルト

デフォルト モードはサーバ モードです。

ドメイン名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。

プルーンングはディセーブルです。

VTP バージョン 2 (v2 モード) はディセーブルです。

コマンド モード VLAN コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VTP モードが透過型である場合、モードおよびドメイン名は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。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。

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。

- スイッチを VTP サーバ モードに戻すには、このコマンドの **no vtp client** および **no vtp transparent** 形式を使用します。
- **vtp server** コマンドは、スイッチがクライアント 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戻さないことを除けば、**no vtp client** または **no vtp transparent** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバのコンフィギュレーションをコピーします。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたは透過モードである場合、スイッチの設定は変更されません。
- 透過モードのスイッチは、VTP に参加しません。透過モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードにあるスイッチで 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スイッチに伝播されます。
- **vtp transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 設定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 モードは透過型に設定してください。
- 拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、その設定は許可されません。
- 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かぎります。



(注) VTP コンフィギュレーション モードの VTP 設定は、適用されたときに VLAN データベースに保存されます。

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、スイッチは非管理ドメイン ステートに置かれます。非管理ドメイン ステートに置かれている間は、ローカル VLAN 設定に変更が生じていてもスイッチは VTP アドパタイズを送信しません。スイッチは、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あと、または **vtp domain** コマンドでドメイン名を設定したあとで、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を **0** にリセットします。スイッチが非管理ドメイン 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ことがありません。

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。

- パスワードでは、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スイッチで一致している必要があります。
- スイッチを非パスワード ステートに戻す場合は、このコマンドの **no vtp password** 形式を使用します。

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 サーバでプルーニングをイネーブルにすると、プルーニングは管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、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 2 (v2 モード) をイネーブルにする場合には、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 スイッチは他のすべての 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 スイッチでバージョン 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 モードで稼動するよう設定する必要があります (**no vtp v2-mode**)。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 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 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、またはトークンリングブリッジリレー機能 (TrBRF) やトークンリング コンセントレータリレー機能 (TrCRF) VLAN メディア タイプを設定している場合には、VTP バージョン 2 (**v2-mode**) をイネーブルにしてください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、VTP バージョン 1 を使用してください。

例 次の例では、スイッチを VTP 透過モードにする方法を示します。

```
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(vlan)# vtp domain OurDomainName
Changing VTP domain name from cisco to OurDomainName
```

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。

```
Switch(vlan)# vtp password private
Setting device VLAN database password to private.
```

次の例では、設定しようとしている新規 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。

```
Switch(vlan)# vtp pruning
Pruning switched ON
```

次の例では、設定しようとしている新規 VLAN データベースで v2 モードをイネーブルにする方法を示します。

```
Switch(vlan)# vtp v2-mode
V2 mode enabled.
```

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。

関連コマンド

コマンド	説明
show vtp status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
switchport trunk pruning	トランキング モードのポートの VLAN プルーンング適格リストを設定します。
vtp (グローバル コンフィギュレーション)	VTP ファイル名、インターフェイス、ドメイン名、およびモードを設定します。



APPENDIX **A**

Catalyst 2960 スイッチ ブートローダ コマンド

この付録では、Catalyst 2960 スイッチのブートローダ コマンドについて説明します。

通常のブートローダ処理中は、ブートローダ コマンドライン プロンプトが表示されません。ブートローダ コマンドラインを使用できるのは、スイッチが手動ブートアップに設定されている場合、Power-on Self-Test (POST; 電源投入時自己診断テスト) DRAM テスト中にエラーが発生した場合、またはオペレーティング システム (破壊された Cisco IOS イメージ) のロード中にエラーが発生した場合です。スイッチのパスワードを忘れた場合にも、ブートローダを使用できます。



(注)

スイッチのデフォルトの設定を使用すると、スイッチに物理的にアクセスするエンドユーザは、スイッチの電源投入時にブートアップ プロセスを中断して新しいパスワードを入力することにより、パスワードを失った状態から回復できます。パスワード回復ディセーブル機能を使用すると、システム管理者は、この機能の一部をディセーブルにし、システムをデフォルト設定に戻すことに同意するだけでユーザがブートアップ プロセスを中断できるようにすることにより、スイッチのパスワードへのアクセスを防止できます。パスワード回復をディセーブルにすることにより、ユーザはブートアップ プロセスを中断してパスワードを変更できますが、コンフィギュレーションファイル (config.text) と VLAN データベース ファイル (vlan.dat) は削除されます。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。

ブートローダには、9600 bps のスイッチ コンソール接続を介してアクセスできます。

スイッチの電源コードを取り外し、電源コードの再接続中に **Mode** ボタンを押します。ポート 1X の上の LED が消灯してから 1 ~ 2 秒後に、**Mode** ボタンを放します。その後、ブートローダの *Switch:* プロンプトが表示されます。ブートローダは低レベルの CPU 初期化および POST を実行し、デフォルトのオペレーティング システム イメージをメモリにロードします。

boot

実行可能イメージをロードおよび起動して、Command-Line Interface (CLI; コマンドライン インターフェイス) を開始するには、**boot** ブートローダ コマンドを使用します。

```
boot [-post | -n | -p |flag] filesystem:/file-url ...
```

シンタックスの説明

-post	(任意) 拡張および総合 Power-on Self-Test (POST; 電源投入時自己診断テスト) によってロードされたイメージを実行します。このキーワードを使用すると、POST の完了に要する時間が長くなります。
-n	(任意) Cisco IOS デバッガのため起動後ただちに一時停止します。
-p	(任意) イメージをロードした直後、JTAG デバッガのために一時停止します。
filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: を使用します。
/file-url	(任意) ブート可能イメージのパス (ディレクトリ) および名前です。各イメージ名はセミコロンで区切ります。

デフォルト

スイッチは、BOOT 環境変数内の情報を使用して、自動的にシステムの起動を試みます。この変数が設定されていない場合、スイッチは、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、最初の実行可能イメージをロードして実行しようとしています。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。

コマンドモード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

引数を何も指定しないで **boot** コマンドを入力した場合、スイッチは、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起動しようとしています。**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起動しようとしています。

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 セッションにのみ適用されます。これらの設定が保存されて、次の起動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では、大文字と小文字が区別されます。

例

次の例では、*new-image.bin* イメージを使用してスイッチを起動する方法を示します。

```
switch: boot flash:/new-images/new-image.bin
```

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。

関連コマンド

コマンド	説明
set	コマンドに BOOT キーワードを追加して、特定のイメージを起動するように BOOT 環境変数を設定します。

cat

1 つまたは複数のファイルの内容を表示するには、**cat** ブートローダ コマンドを使用します。

```
cat filesystem:/file-url ...
```

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: を使用します。
<i>/file-url</i>	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。

コマンドモード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
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。

例

次の例では、サンプル出力で 2 つのファイルの内容を表示する方法を示します。

```
switch: cat flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: LAYER_2|MIN_DRAM_MEG=64
image_family:switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

関連コマンド

コマンド	説明
more	1 つまたは複数のファイルの内容を表示します。
type	1 つまたは複数のファイルの内容を表示します。

copy

ファイルをコピー元からコピー先にコピーするには、**copy** ブートローダ コマンドを使用します。

```
copy [-b block-size] filesystem:/source-file-url filesystem:/destination-file-url
```

シンタックスの説明

-b <i>block-size</i>	(任意) このオプションは、内部開発およびテスト専用です。
<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: を使用します。
<i>/source-file-url</i>	コピー元のパス (ディレクトリ) およびファイル名です。
<i>/destination-file-url</i>	コピー先のパス (ディレクトリ) およびファイル名です。

デフォルト

デフォルトのブロック サイズは 4 KB です。

コマンド モード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名および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 45 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、およびコロンは使用できません。

指定できるファイル名は最大 45 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、および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る必要があります。

例

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。

```
switch: copy flash:test1.text flash:test4.text
.
```

File "flash:test1.text" successfully copied to "flash: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。

関連コマンド

コマンド	説明
delete	指定されたファイル システムから 1 つまたは複数のファイルを削除します。

delete

指定されたファイル システムから 1 つまたは複数のファイルを削除するには、**delete** ブートローダ コマンドを使用します。

delete *filesystem:/file-url ...*

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボードフラッシュ デバイスに対して flash: を使用します。
<i>/file-url</i>	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。

コマンド モード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。各ファイルを削除する前に、確認を求めるプロンプトが表示されます。

例

次の例では、2 つのファイルを削除します。

```
switch: delete flash:test2.text flash:test5.text
Are you sure you want to delete "flash:test2.text" (y/n)?y
File "flash:test2.text" deleted
Are you sure you want to delete "flash:test5.text" (y/n)?y
File "flash:test2.text" deleted
```

ファイルが削除されたかどうかを確認するには、**dir flash:** ブートローダ コマンドを入力します。

関連コマンド

コマンド	説明
copy	コピー元からコピー先にファイルをコピーします。

dir

指定されたファイル システム上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、**dir** ブートローダ コマンドを使用します。

dir filesystem:/file-url ...

シンタックスの説明	filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: を使用します。
	/file-url	(任意) 内容を表示するパス (ディレクトリ) およびディレクトリ名です。ディレクトリ名はスペースで区切ります。

コマンド モード ブートローダ

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン ディレクトリ名は、大文字と小文字が区別されます。

例 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。

```
switch: dir flash:
Directory of flash:/

   3  -rwx      1839   Mar 01 2002 00:48:15  config.text
  11  -rwx      1140   Mar 01 2002 04:18:48  vlan.dat
  21  -rwx         26   Mar 01 2002 00:01:39  env_vars
   9  drwx       768   Mar 01 2002 23:11:42  html
  16  -rwx     1037   Mar 01 2002 00:01:11  config.text
  14  -rwx     1099   Mar 01 2002 01:14:05  homepage.htm
  22  -rwx         96   Mar 01 2002 00:01:39  system_env_vars
  17  drwx       192   Mar 06 2002 23:22:03  imnage-name
```

15998976 bytes total (6397440 bytes free)

表 A-1 に、表示されるフィールドの説明を示します。

表 A-1 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
-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 : 読み込み可能 • w : 書き込み可能 • x : 実行可能
1644045	ファイルのサイズ
<日付>	最終変更日
env_vars	ファイル名

関連コマンド

コマンド	説明
mkdir	1 つまたは複数のディレクトリを作成します。
rmdir	1 つまたは複数のディレクトリを削除します。

flash_init

フラッシュ ファイル システムを初期化するには、**flash_init** ブートローダ コマンドを使用します。

flash_init

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト フラッシュ 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。

コマンド モード ブートローダ

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン フラッシュ ファイル システムは、通常の起動プロセス中に自動的に初期化されます。
このコマンドは、フラッシュ 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。

format

指定されたファイル システムをフォーマットし、そのファイル システム内のすべてのデータを破棄するには、**format** ブートローダ コマンドを使用します。

format *filesystem:*

シンタックスの説明

filesystem: フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して **flash:** を使用します。

コマンド モード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン



注意

このコマンドは慎重に使用してください。ファイル システム内のすべてのデータが破棄され、システムが使用不可能になります。

fsck

ファイル システムの一貫性を確認するには、**fsck** ブートローダ コマンドを使用します。

fsck [-test | -f] filesystem:

シンタックスの説明	
-test	(任意) ファイル システム コードを初期化し、フラッシュ メモリ上で新しい POST を実行します。ファイル システムを構成するバイトごとに、広範なメモリ テストを実行します (メモリは破壊されません)。
-f	(任意) ファイル システム コードを初期化し、高速ファイル一貫性チェックを実行します。フラッシュ セクタ内の Cyclic Redundancy Check (CRC; 巡回冗長検査) は実行されません。
filesystem:	フラッシュ ファイル システムのエリアスです。システム ボードフラッシュ デバイスに対して flash: を使用します。

デフォルト ファイル システム チェックは実行されません。

コマンド モード ブートローダ

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン 進行中のファイル システム一貫性チェックを停止するには、スイッチの電源を切断してから、電源を再接続します。

例 次の例では、フラッシュ メモリ上で広範なファイル システム チェックを実行する方法を示します。
switch: fsck -test flash:

help

使用可能なコマンドを表示するには、**help** ブートローダ コマンドを使用します。

help

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

疑問符 (?) を使用して、使用可能なブートローダ コマンドのリストを表示することもできます。

memory

メモリ ヒープ使用率情報を表示するには、**memory** ブートローダ コマンドを使用します。

memory

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

コマンド モード ブートローダ

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

例 次の例では、メモリ ヒープ使用率情報を表示する方法を示します。

```
switch: memory
Text: 0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext: 0x00000000 - 0x00000000 (0x00000000 bytes)
Data: 0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss: 0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Heap: 0x00756f98 - 0x00800000 (0x000a9068 bytes)
```

```
Bottom heap utilization is 22 percent.
Top heap utilization is 0 percent.
Total heap utilization is 22 percent.
Total bytes: 0xa9068 (692328)
Bytes used: 0x26888 (157832)
Bytes available: 0x827e0 (534496)
```

```
Alternate heap utilization is 0 percent.
Total alternate heap bytes: 0x6fd000 (7327744)
Alternate heap bytes used: 0x0 (0)
Alternate heap bytes available: 0x6fd000 (7327744)
```

表 A-2 に、表示されるフィールドの説明を示します。

表 A-2 memory のフィールドの説明

フィールド	説明
Text	テキスト記憶領域の先頭および末尾アドレス。
Rotext	読み取り専用テキスト記憶領域の先頭および末尾アドレス。データ セグメントのこの部分は、Text エントリとともにグループ化されます。
Data	データ セグメント記憶領域の先頭および末尾アドレス。
Bss	Block Started by Symbol (Bss) 記憶領域から始まるブロックの先頭および末尾アドレス。ゼロに初期化されています。
Heap	メモリの割り当ておよび解放が動的に行われるメモリ領域の先頭および末尾アドレス。

mkdir

指定されたファイル システムに 1 つまたは複数のディレクトリを新規作成するには、**mkdir** ブートローダ コマンドを使用します。

```
mkdir filesystem:/directory-url ...
```

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボードフラッシュ デバイスに対して flash: を使用します。
<i>/directory-url</i>	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。

コマンドモード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ディレクトリ名は、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 45 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、および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。

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

次の例では、2 つのディレクトリを作成する方法を示します。

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

ディレクトリが作成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。

関連コマンド

コマンド	説明
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します。
rmdir	指定されたファイル システムから 1 つまたは複数のディレクトリを削除します。

more

1 つまたは複数のファイルの内容を表示するには、**more** ブートローダ コマンドを使用します。

more filesystem:/file-url ...

シンタックスの説明	filesystem:	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して 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。

コマンド モード ブートローダ

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン ファイル名およびディレクトリ名では、大文字と小文字が区別されます。
 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。

例 次の例では、2 つのファイルの内容を表示する方法を示します。

```
switch: more flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name
c2960-lanbase-mz.122-25.FX
image_name: image-name.bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: LAYER_2|MIN_DRAM_MEG=64switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

関連コマンド	コマンド	説明
	cat	1 つまたは複数のファイルの内容を表示します。
	type	1 つまたは複数のファイルの内容を表示します。

rename

ファイルの名前を変更するには、**rename** ブートローダ コマンドを使用します。

```
rename filesystem:/source-file-url filesystem:/destination-file-url
```

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: 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。

コマンド モード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名および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 45 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、およびコロンは使用できません。

指定できるファイル名は最大 45 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、およびコロンは使用できません。

例

次の例では、ファイル *config.text* の名前を *config1.text* に変更します。

```
switch: rename flash:config.text flash:config1.text
```

ファイル名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。

関連コマンド

コマンド	説明
copy	コピー元からコピー先にファイルをコピーします。

reset

システムのハードリセットを実行するには、**reset** ブートローダ コマンドを使用します。ハードリセットを行うと、スイッチ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

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

コマンド モード ブートローダ

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

例 次の例では、システムをリセットする方法を示します。

```
switch: reset  
Are you sure you want to reset the system (y/n)?y  
System resetting...
```

関連コマンド	コマンド	説明
	boot	実行可能イメージをロードおよび起動して、コマンドライン インターフェイスを開始します。

rmdir

指定されたファイル システムから 1 つまたは複数の空のディレクトリを削除するには、**rmdir** ブートローダ コマンドを使用します。

```
rmdir filesystem:/directory-url ...
```

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボード フラッシュ デバイスに対して flash: を使用します。
<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。

コマンドモード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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、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。

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が表示されます。

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。

```
switch: rmdir flash: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。

関連コマンド

コマンド	説明
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します。
mkdir	指定されたファイル システムに 1 つまたは複数のディレクトリを新規作成します。

set

ブートローダまたはスイッチ上で稼動している他のソフトウェアを制御するために使用できる環境変数を設定したり、表示するには、**set** ブートローダ コマンドを使用します。

set *variable value*

シンタックスの説明

<i>variable value</i>	<i>variable</i> および <i>value</i> には、次に示すキーワードのいずれかを使用します。
	MANUAL_BOOT : スイッチを自動で起動するか、または手動で起動するかを決定します。 有効値は 1、yes、0、および no です。no または 0 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ようとします。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スイッチ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です。 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、最初に見つかった実行可能イメージをロードして実行しようとします。BOOT 環境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い場合は、システムはフラッシュ ファイル システムで最初に見つかったブート ファイルを起動しようとします。
	ENABLE_BREAK : コンソール上の Break キーを使用して自動起動プロセスを中断できるかどうかを決定します。 有効値は 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 キーを押して、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です。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される文字列です。
	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です。
	BAUD rate : コンソールで使用される速度 (ビット/秒単位) です。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かぎり、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。指定できる範囲は 0 ~ 4294967295 bps 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。
	HELPER_CONFIG_FILE filesystem:/file-url : Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前です。この名前が設定されていない場合は、CONFIG_FILE 環境変数で指定されたファイルが、ロードされるすべてのバージョンの Cisco IOS (ヘルパー イメージを含む) で使用されます。この変数は、内部開発およびテスト専用です。

デフォルト

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 : switch:

CONFIG_FILE : config.text

BAUD : 9600 bps

HELPER_CONFIG_FILE : デフォルト値はありません (ヘルパー コンフィギュレーション ファイルは指定されません)。

SWITCH_NUMBER : 1

SWITCH_PRIORITY : 1



(注)

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 システムに保存されています。これらのファイルの各行に、環境変数名と等号、そのあとに変数の値が格納されています。このファイルに表示されていなければ、その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 " ") に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。

コマンドモード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

値が設定された環境変数は、フラッシュ ファイル システム外のフラッシュ メモリに保存されています。

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。

HELPER_CONFIG_FILE 環境変数は、**boot helper-config-file 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。

HELPER_CONFIG_FILE 環境変数は、**boot helper-config-file 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。

ブートローダのプロンプト スtring (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

次の例では、ブートローダのプロンプトを確認する方法を示します。

```
switch: set PS1 loader:  
loader:
```

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。

関連コマンド

コマンド	説明
unset	1 つまたは複数の環境変数を元の設定に戻します。

type

1 つまたは複数のファイルの内容を表示するには、**type** ブートローダ コマンドを使用します。

type *filesystem:/file-url ...*

シンタックスの説明

<i>filesystem:</i>	フラッシュ ファイル システムのエイリアスです。システム ボードフラッシュ デバイスに対して flash: を使用します。
<i>/file-url</i>	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。

コマンドモード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ファイル名およびディレクトリ名では、大文字と小文字が区別されます。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。

例

次の例では、2 つのファイルの内容を表示する方法を示します。

```
switch: type flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: LAYER_2|MIN_DRAM_MEG=64switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

関連コマンド

コマンド	説明
cat	1 つまたは複数のファイルの内容を表示します。
more	1 つまたは複数のファイルの内容を表示します。

unset

1 つまたは複数の環境変数をリセットするには、**unset** ブートローダ コマンドを使用します。

unset *variable* ...

シンタックスの説明

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 : スイッチを自動で起動するか、または手動で起動するかを決定します。

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、最初に見つかった実行可能イメージをロードして実行しようとします。**BOOT** 環境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い場合は、システムはフラッシュ ファイル システムで最初に見つかったブート 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起動プロセスを中断できるかどうかを決定します。

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です。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される文字列です。

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かぎり、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。

HELPER_CONFIG_FILE : Cisco IOS ヘルパー イメージで使用されるコンフィギュレーション ファイルの名前をリセットします。この名前が設定されていない場合は、**CONFIG_FILE** 環境変数で指定されたファイルが、ロードされるすべてのバージョンの Cisco IOS (ヘルパー イメージを含む) で使用されます。この変数は、内部開発およびテスト専用です。

コマンド モード

ブートローダ

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

通常的环境中では、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。

HELPER_CONFIG_FILE 環境変数は、**no boot helper-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。

ブートローダのプロンプト スtring (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

次の例では、プロンプト スtring を元の設定にリセットする方法を示します。

```
switch: unset PS1
switch:
```

関連コマンド

コマンド	説明
set	環境変数を設定または表示します。

version

ブートローダのバージョンを表示するには、**version** ブートローダ コマンドを使用します。

version

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

コマンド モード ブートローダ

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

例 次の例では、ブートローダのバージョンを表示する方法を示します。

```
switch: version  
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25)FX  
Compiled Wed 05-Mar-08 10:11 by engineer
```

■ version



APPENDIX **B**

Catalyst 2960 スイッチ デバッグ コマンド

この付録では、Catalyst2960 スイッチで使用するために作成または変更された **debug** 特権 EXEC コマンドについて説明します。これらのコマンドは、インターネットワーキングの問題の診断および解決に役立ちます。使用する場合には、必ずシスコのテクニカル サポート担当者の指示に従ってください。



注意

デバッグ出力には、CPU プロセスで高いプライオリティが与えられるので、システムが使用不能になる可能性があります。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。**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。

debug auto qos

Automatic Quality of Service (auto-QoS) 機能の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



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、キーワードと引数はありません。

デフォルト

auto-QoS デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

auto-QoS がイネーブルのときに自動的に生成される QoS (Quality of Service) 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。

例

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。

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip cisco-phone

21:29:41: mls qos map cos-dscp 0 8 16 26 32 46 48 56
21:29:41: mls qos
21:29:42: no mls qos srr-queue input cos-map
21:29:42: no mls qos srr-queue output cos-map
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 3 0
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 2 1
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 1 2
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
```

```

21:29:43: mls qos srr-queue input cos-map queue 2 threshold 3 3 5
21:29:43: mls qos srr-queue output cos-map queue 1 threshold 3 5
21:29:43: mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
21:29:44: mls qos srr-queue output cos-map queue 3 threshold 3 2 4
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 2 1
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 3 0
21:29:44: no mls qos srr-queue input dscp-map
21:29:44: no mls qos srr-queue output dscp-map
21:29:44: mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 32
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
21:29:48: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 1 8
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
21:29:49: no mls qos srr-queue input priority-queue 1
21:29:49: no mls qos srr-queue input priority-queue 2
21:29:50: mls qos srr-queue input bandwidth 90 10
21:29:50: no mls qos srr-queue input buffers
21:29:50: mls qos queue-set output 1 buffers 10 10 26 54
21:29:50: interface GigabitEthernet0/1
21:29:50: mls qos trust device cisco-phone
21:29:50: mls qos trust cos
21:29:50: no queue-set 1
21:29:50: srr-queue bandwidth shape 10 0 0 0
21:29:50: srr-queue bandwidth share 10 10 60 20

```

関連コマンド

コマンド	説明
auto qos voip	QoS ドメイン内で Voice over IP (VoIP) の auto-QoS を設定します。
show auto qos	auto-QoS 機能によって生成された初期設定を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug backup

Flex Link バックアップ インターフェイスのデバッグをイネーブルにするには、**debug backup** 特権 EXEC 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 backup {all | errors | events | vlan-load-balancing}

no debug backup {all | errors | events | vlan-load-balancing}

シンタックスの説明

all	バックアップ インターフェイスのデバッグ メッセージをすべて表示します。
errors	バックアップ インターフェイスのエラーまたは例外デバッグ メッセージを表示します。
events	バックアップ インターフェイスのイベント デバッグ メッセージを表示します。
vlan-load-balancing	バックアップ インターフェイスの VLAN ロード バランシングを表示します。

デフォルト

バックアップ インターフェイス デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(37)SE	vlan-load-balancing キーワードが追加されました。
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug backup コマンドは、**no debug backup** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug cisp

Client Information Signalling Protocol (CISP) に対応したインターフェイス上で発生したメッセージ交換とイベントのデバッグをイネーブルにするには、**debug cisp** 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 cisp [all | errors | events | packets | sync]

no debug cisp [initialization | interface-configuration | rpc]

シンタックスの説明

all	すべての CISP デバッグ メッセージを表示します。
errors	CISP デバッグ メッセージを表示します。
events	CISP イベント デバッグ メッセージを表示します。
packets	CISP パケット デバッグ メッセージを表示します。
sync	CISP 運用同期デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol (CISP) をイネーブルにします。
dot1x credentials (グローバル コンフィギュレーション) profile	サブリカント スイッチのプロファイルを設定します。
show cisp	特定のインターフェイスの CISP 情報を表示します。

debug cluster

クラスタ固有イベントのデバッグをイネーブルにするには、**debug cluster** 特権 EXEC 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 cluster {discovery | events | extended | hsrp | http | ip [packet] | members | nat |
neighbors | platform | snmp | vqpxy}
```

```
no debug cluster {discovery | events | extended | hsrp | http | ip [packet] | members | nat
| neighbors | platform | snmp | vqpxy}
```

シンタックスの説明

discovery	クラスタ ディスカバリ デバッグ メッセージを表示します。
events	クラスタ イベント デバッグ メッセージを表示します。
extended	拡張ディスカバリ デバッグ メッセージを表示します。
hsrp	Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) デバッグ メッセージを表示します。
http	HTTP デバッグ メッセージを表示します。
ip [packet]	IP またはトランスポート パケット デバッグ メッセージを表示します。
members	クラスタ メンバー デバッグ メッセージを表示します。
nat	Network Address Translation (NAT; ネットワーク アドレス変換) デバッグ メッセージを表示します。
neighbors	クラスタ ネイバー デバッグ メッセージを表示します。
platform	プラットフォーム特定クラスタ デバッグ メッセージを表示します。
snmp	SNMP (簡易ネットワーク管理プロトコル) デバッグ メッセージを表示します。
vqpxy	VLAN (仮想 LAN) Query Protocol (VQP) プロキシデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クラスタ コマンド スイッチ上でのみ利用できます。

undebug cluster コマンドは、**no debug cluster** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show cluster	スイッチが属するクラスタのステータスおよびサマリーを表示します。
show cluster candidates	コマンド スイッチ上で入力された場合に候補スイッチのリストを表示します。
show cluster members	コマンド スイッチ上で実行された場合にクラスタ メンバーに関する情報を表示します。

debug dot1x

IEEE 802.1x 認証機能のデバッグをイネーブルにするには、**debug dot1x** 特権 EXEC 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 dot1x {all | errors | events | feature | packets | registry | state-machine}

no debug dot1x {all | errors | events | feature | packets | registry | state-machine}

シンタックスの説明

all	すべての IEEE 802.1x 認証デバッグ メッセージを表示します。
errors	IEEE 802.1x エラー デバッグ メッセージを表示します。
events	IEEE 802.1x イベント デバッグ メッセージを表示します。
feature	IEEE 802.1x 機能のデバッグ メッセージを表示します。
packets	IEEE 802.1x パケット デバッグ メッセージを表示します。
registry	IEEE 802.1x レジストリ呼び出しのデバッグ メッセージを表示します。
state-machine	ステート マシン関連イベント デバッグ メッセージを表示します。



(注)

redundancy キーワードは、コマンドラインのヘルプ スtringには表示されますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SEE	feature キーワードが追加されました。

使用上のガイドライン

undebug dot1x コマンドは、**no debug dot1x** コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	イネーブルになっているデバッグタイプに関する情報を表示します。
<code>show dot1x</code>	スイッチ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します。

debug dtp

この Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) アクティビティのデバッグをイネーブルにするには、**debug dtp** 特権 EXEC 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 dtp {aggregation | all | decision | events | oserrs | packets | queue | states | timers}
```

```
no debug dtp {aggregation | all | decision | events | oserrs | packets | queue | states | timers}
```

シンタックスの説明

aggregation	DTP ユーザ メッセージ アグリゲーション デバッグ メッセージを表示します。
all	すべての DTP デバッグ メッセージを表示します。
decision	DTP 決定テーブル デバッグ メッセージを表示します。
events	DTP イベント デバッグ メッセージを表示します。
oserrs	DTP オペレーティングシステム関連エラー デバッグ メッセージを表示します。
packets	DTP パケット処理デバッグ メッセージを表示します。
queue	DTP パケット キューイング デバッグ メッセージを表示します。
states	DTP ステート遷移デバッグ メッセージを表示します。
timers	DTP タイマー イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug dtp コマンドは、**no debug dtp** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show dtp	スイッチまたは指定されたインターフェイスの DTP 情報を表示します。

debug eap

Extensible Authentication Protocol (EAP) のアクティビティをデバッグするには、**debug eap** 特権 EXEC 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 dot1x {all | authenticator | errors | events | md5 | packets | peer | sm}
```

```
no debug dot1x {all | authenticator | errors | events | md5 | packets | peer | sm}
```

シンタックスの説明

all	EAP デバッグ メッセージをすべて表示します。
authenticator	オーセンティケータ デバッグ メッセージを表示します。
errors	EAP エラー デバッグ メッセージを表示します。
events	EAP イベント デバッグ メッセージを表示します。
md5	EAP-MD5 デバッグ メッセージを表示します。
packets	EAP パケット デバッグ メッセージを表示します。
peer	EAP ピア デバッグ メッセージを表示します。
sm	EAP ステート マシン関連イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SEE	このコマンドが追加されました。

使用上のガイドライン

undebug dot1x コマンドは、**no debug dot1x** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show eap	スイッチまたは特定のポートの EAP のレジストレーション情報およびセッション情報を表示します。

debug etherchannel

EtherChannel/Port Aggregation Protocol (PAgP; ポート集約プロトコル) シムのデバッグをイネーブルにするには、**debug etherchannel** 特権 EXEC コマンドを使用します。このシムは、PAgP ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール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。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**]

シンタックスの説明

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) 主な EtherChannel イベント メッセージをデバッグします。
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。



(注)

linecard キーワードは、コマンドラインのヘルプ スtring には表示されますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

undebug etherchannel コマンドは、**no debug etherchannel** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグタイプに関する情報を表示します。
show etherchannel	チャンネルの EtherChannel 情報を表示します。

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、**debug ilpower** 特権 EXEC 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 ilpower {cdp | controller | event | ha | port | powerman | registries}
```

```
no debug ilpower {cdp | controller | event | ha | port | powerman | registries}
```

シンタックスの説明

cdp	PoE Cisco Discovery Protocol (CDP) デバッグ メッセージを表示します。
controller	PoE コントローラ 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。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応スイッチのみでサポートされています。

デバッグをイネーブルにすると、スイッチでのみデバッグがイネーブルになります。

関連コマンド

コマンド	説明
show controllers power inline	指定した PoE コントローラのレジスタの値を表示します。
show power inline	指定した PoE ポートまたはすべての PoE ポートの電源ステータスを表示します。

debug interface

インターフェイス関連のアクティビティのデバッグをイネーブルにするには、**debug interface** 特権 EXEC 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 interface {interface-id | null interface-number | port-channel port-channel-number |
  vlan vlan-id}
```

```
no debug interface {interface-id | null interface-number | port-channel port-channel-number |
  vlan vlan-id}
```

シンタックスの説明

<i>interface-id</i>	タイプ スイッチ番号/モジュール番号/ポート (例 : gigabitethernet 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 <i>interface-number</i>	ヌル 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>interface-number</i> 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 ~ 6 です。
vlan <i>vlan-id</i>	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 <i>vlan id</i> の 範囲は 1 ~ 4094 です。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

undebug interface コマンドは、**no debug interface** コマンドと同じです。

■ debug interface

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show etherchannel	チャンネルの EtherChannel 情報を表示します。

debug ip dhcp snooping

DHCP スヌーピングのデバッグをイネーブルにするには、**debug ip dhcp snooping** 特権 EXEC 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 ip dhcp snooping {mac-address | agent | event | packet}
```

```
no debug ip dhcp snooping {mac-address | agent | event | packet}
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

<i>mac-address</i>	指定された MAC (メディア アクセス制御) アドレスを持つ DHCP パケットのデバッグ メッセージを表示します。
agent	DHCP スヌーピング エージェントのデバッグ メッセージを表示します。
event	DHCP スヌーピング イベントのデバッグ メッセージを表示します。
packet	DHCP スヌーピングのデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug ip dhcp snooping コマンドは、**no debug ip dhcp snooping** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug ip igmp filter

Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) フィルタ イベントのデバッグをイネーブルにするには、**debug ip igmp filter** 特権 EXEC 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 ip igmp filter

no debug ip igmp filter

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug ip igmp filter コマンドは、**no debug ip igmp filter** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug ip igmp max-groups

IGMP 最大グループ イベントのデバッグをイネーブルにするには、**debug ip igmp max-groups** 特権 EXEC 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 ip igmp max-groups

no debug ip igmp max-groups

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **undebug ip igmp max-groups** コマンドは、**no debug ip igmp max-groups** コマンドと同じです。

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug ip igmp snooping

インターネット グループ管理プロトコル (IGMP) スヌーピング アクティビティのデバッグをイネーブルにするには、**debug ip igmp snooping** 特権 EXEC 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 ip igmp snooping [group | management | querier | router | timer]

no debug ip igmp snooping [group | management | querier | router | timer]

シンタックスの説明

group	(任意) IGMP スヌーピング グループ アクティビティのデバッグ メッセージを表示します。
management	(任意) IGMP スヌーピング管理アクティビティのデバッグ メッセージを表示します。
querier	(任意) IGMP スヌーピング クエリア デバッグ メッセージを表示します。
router	(任意) IGMP スヌーピング ルータ アクティビティのデバッグ メッセージを表示します。
timer	(任意) IGMP スヌーピング タイマー イベントのデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug ip igmp snooping コマンドは、**no debug ip igmp snooping** コマンドと同じです。

関連コマンド

コマンド	説明
debug platform ip igmp snooping	プラットフォームに依存する IGMP スヌーピング アクティビティに関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug lacp

Link Aggregation Control Protocol (LACP) のアクティビティのデバッグをイネーブルにするには、**debug lacp** 特権 EXEC 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 lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

シンタックスの説明

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 有限ステート マシン デバッグ 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) LACP パケット デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug lacp コマンドは、**no debug lacp** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show lacp	LACP チャネル グループ情報を表示します。

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、**debug lldp packets** 特権 EXEC 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 lldp packets

no debug lldp packets



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug lldp packets コマンドは、**no debug lldp packets** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug mac-notification

MAC（メディア アクセス制御）通知イベントのデバッグをイネーブルにするには、**debug mac-notification** 特権 EXEC 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 mac-notification

no debug mac-notification

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **undebug mac-notification** コマンドは、**no debug mac-notification** コマンドと同じです。

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show mac address-table notification	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 アドレス通知情報を表示します。

debug matm

プラットフォーム独立 MAC（メディア アクセス制御）アドレス管理のデバッグをイネーブルにするには、**debug matm** 特権 EXEC 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 matm

no debug matm

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug matm コマンドは、**no debug matm** コマンドと同じです。

関連コマンド

コマンド	説明
debug platform matm	プラットフォームに依存する MAC アドレス管理に関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug matm move update

MAC (メディア アクセス制御) アドレス テーブル移行更新メッセージ処理のデバッグをイネーブルにするには、**debug matm move update** 特権 EXEC コマンドを使用します。

debug matm move update

no debug matm move update



(注) このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

undebug matm move update コマンドは、**no debug matm move update** コマンドと同じです。

関連コマンド

コマンド	説明
mac address-table move update {receive transmit}	スイッチに MAC アドレス テーブル移行更新機能を設定します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。

debug monitor

Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 機能のデバッグをイネーブルにするには、**debug monitor** 特権 EXEC 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 monitor {all | errors | idb-update | info | list | notifications | platform | requests | snmp}

no debug monitor {all | errors | idb-update | info | list | notifications | platform | requests | snmp}

シンタックスの説明

all	すべての SPAN デバッグ メッセージを表示します。
errors	詳細 SPAN エラー デバッグ メッセージを表示します。
idb-update	SPAN Interface Description Block (IDB; インターフェイス デスクリプション ブロック) 更新トレース デバッグ メッセージを表示します。
info	SPAN 情報追跡デバッグ メッセージを表示します。
list	SPAN ポートおよび VLAN リスト追跡デバッグ メッセージを表示します。
notifications	SPAN 通知デバッグ メッセージを表示します。
platform	SPAN プラットフォーム追跡デバッグ メッセージを表示します。
requests	SPAN 要求デバッグ メッセージを表示します。
snmp	SPAN および SNMP (簡易ネットワーク管理プロトコル) 追跡デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug monitor コマンドは、**no debug monitor** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show monitor	スイッチ上の SPAN および Remote SPAN (RSPAN) セッションについてのすべての情報を表示します。

debug mvrdbg

Multicast VLAN Registration (MVR) のデバッグをイネーブルにするには、**debug mvrdbg** 特権 EXEC 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 mvrdbg {all | events | igmpsn | management | ports}
```

```
no debug mvrdbg {all | events | igmpsn | management | ports}
```



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

all	MVR アクティビティ デバッグ メッセージをすべて表示します。
events	MVR イベント処理デバッグ メッセージを表示します。
igmpsn	MVR インターネット グループ管理プロトコル (IGMP) スヌーピング アクティビティ デバッグ メッセージを表示します。
management	MVR 管理アクティビティ デバッグ メッセージを表示します。
ports	MVR ポート デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug mvrdbg コマンドは、**no debug mvrdbg** コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	イネーブルになっているデバッグタイプに関する情報を表示します。
<code>show mvr</code>	現在の MVR 設定を表示します。

debug nmsp

スイッチ上で Network Mobility Services Protocol (NMSP; ネットワーク モビリティ サービス プロトコル) のデバッグをイネーブルにするには、**debug nmsp** 特権 EXEC コマンドを入力します。このコマンドを使用できるのは、スイッチで暗号化ソフトウェア イメージが実行されている場合だけです。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 nmsp {all | connection | error | event | packet | rx | tx}

no debug nmsp



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebug nmsp コマンドは、**no debug nmsp** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show nmsp	NMSP 情報を表示します。

debug nvram

NVRAM（不揮発性 RAM）のアクティビティのデバッグをイネーブルにするには、**debug nvram** 特権 EXEC 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 nvram

no debug nvram

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **undebug nvram** コマンドは、**no debug nvram** コマンドと同じです。

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug pagp

ポート集約プロトコル (PAgP) のアクティビティのデバッグをイネーブルにするには、**debug pagp** 特権 EXEC 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 pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

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 有限ステート マシン デバッグ 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) PAgP パケット デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(46)SE	dual-active キーワードが追加されました。

使用上のガイドライン

undebug pagp コマンドは、**no debug pagp** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show pagp	PAgP チャネル グループ情報を表示します。

debug platform acl

Access Control List (ACL; アクセス コントロール リスト) マネージャのデバッグをイネーブルにするには、**debug platform acl** 特権 EXEC 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 platform acl {all | exit | label | main | warn}
```

```
no debug platform acl {all | exit | label | main | warn}
```

シンタックスの説明

all	ACL マネージャ デバッグ メッセージをすべて表示します。
exit	ACL 終了関連デバッグ メッセージを表示します。
label	ACL ラベル関連デバッグ メッセージを表示します。
main	主な、または重要な ACL デバッグ メッセージを表示します。
warn	ACL 警告関連デバッグ メッセージを表示します。



(注) **racl**、**stack**、**vacl**、および **vmap** キーワードはコマンドラインのヘルプ スtring に表示されますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform acl コマンドは、**no debug platform acl** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform backup interface

Flex Link プラットフォーム バックアップ インターフェイスのデバッグをイネーブルにするには、**debug platform backup interface** 特権 EXEC 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 platform backup interface

no debug platform backup interface



(注)

このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

プラットフォーム バックアップ インターフェイス デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform backup interface コマンドは、**no platform debug backup interface** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform cisp

Client Information Signalling Protocol (CISP) に対応した 1 つまたは複数のインターフェイスが装備されているスイッチのプラットフォーム レベルでのデバッグをイネーブルにするには、**debug platform cisp** 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 platform cisp [initialization | interface-configuration | rpc]

no debug platform cisp [initialization | interface-configuration | rpc]

シンタックスの説明	initialization	CISP 初期化シーケンスのデバッグをイネーブルにします。
	interface-configuration	CISP 設定のデバッグをイネーブルにします。
	rpc	CISP RPC 要求のデバッグをイネーブルにします。

デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン デバッグをイネーブルにすると、スタック マスター上でのみデバッグがイネーブルになります。スタック メンバーのデバッグをイネーブルにするには、**session switch-number** 特権 EXEC コマンドを使用してスタック マスターからセッションを開始し、スタック メンバーのコマンドライン プロンプトで debug コマンドを入力します。また、スタック マスター スイッチ上で **remote command stack-member-number <line>** 特権 EXEC コマンドを使用すると、最初にセッションを開始せずにメンバー スイッチのデバッグをイネーブルにすることができます。

関連コマンド	コマンド	説明
	cisp enable	Client Information Signalling Protocol (CISP) をイネーブルにします。
	dot1x credentials (グローバル コンフィギュレーション) profile	サブリカント スイッチのプロファイルを設定します。
	show cisp	特定のインターフェイスの CISP 情報を表示します。

debug platform cpu-queues

プラットフォーム CPU 受信キューのデバッグをイネーブルにするには、**debug platform cpu-queues** 特権 EXEC 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 platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
  igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | software-fwd-q
  | stp-q}
```

```
no debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
  igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | software-fwd-q
  | stp-q}
```

シンタックスの説明

broadcast-q	ブロードキャスト キューによって受信されたパケットに関するデバッグ メッセージを表示します。
cbt-to-spt-q	core-based tree to shortest-path tree (cbt-to-spt) キューによって受信されたパケットに関するデバッグ メッセージを表示します。
cpuhub-q	CPU ハートビート キューによって受信されたパケットに関するデバッグ メッセージを表示します。
host-q	ホスト キューによって受信されたパケットに関するデバッグ メッセージを表示します。
icmp-q	Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) キューによって受信されたパケットに関するデバッグ メッセージを表示します。
igmp-snooping-q	インターネット グループ管理プロトコル (IGMP) スヌーピング キューによって受信されたパケットに関するデバッグ メッセージを表示します。
layer2-protocol-q	レイヤ 2 プロトコル キューによって受信されたパケットに関するデバッグ メッセージを表示します。
logging-q	ロギング キューによって受信されたパケットに関するデバッグ メッセージを表示します。
remote-console-q	リモート コンソール キューによって受信されたパケットに関するデバッグ メッセージを表示します。
software-fwd-q	ソフトウェア フォワーディング キューによって受信されたパケットをデバッグします。
stp-q	Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) キューによって受信されたパケットをデバッグします。



(注) **routing-protocol-Q** および **rpffail-q** 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ていますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン `undebg platform cpu-queues` コマンドは、`no debug platform cpu-queues` コマンドと同じです。

関連コマンド	コマンド	説明
	<code>show debugging</code>	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform dot1x

IEEE 802.1x イベントのデバッグをイネーブルにするには、**debug platform dot1x** 特権 EXEC 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 platform dot1x {initialization | interface-configuration | rpc}

no debug platform dot1x {initialization | interface-configuration | rpc}

シンタックスの説明

initialization	IEEE 802.1x 認証初期化シーケンス デバッグ メッセージを表示します。
interface-configuration	IEEE 802.1x インターフェイス コンフィギュレーション関連デバッグ メッセージを表示します。
rpc	IEEE 802.1x Remote Procedure Call (RPC) 要求デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform dot1x コマンドは、**no debug platform dot1x** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform etherchannel

プラットフォームに依存する EtherChannel イベントのデバッグをイネーブルにするには、**debug platform etherchannel** 特権 EXEC 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 platform etherchannel {init | link-up | rpc | warnings}
```

```
no debug platform etherchannel {init | link-up | rpc | warnings}
```

シンタックスの説明

init	EtherChannel モジュール初期化デバッグ メッセージを表示します。
link-up	EtherChannel リンクアップおよびリンクダウンに関連したデバッグ メッセージを表示します。
rpc	EtherChannel Remote Procedure Call (RPC) デバッグ メッセージを表示します。
warnings	EtherChannel 警告デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform etherchannel コマンドは、**no debug platform etherchannel** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform forw-tcam

フォワーディング Ternary Content Addressable Memory (TCAM) マネージャのデバッグをイネーブルにするには、**debug platform forw-tcam** 特権 EXEC 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 platform forw-tcam [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

no debug platform forw-tcam [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

シンタックスの説明

adjustment	(任意) TCAM マネージャ調整デバッグ メッセージを表示します。
allocate	(任意) TCAM マネージャ割り当てデバッグ メッセージを表示します。
audit	(任意) TCAM マネージャ監査メッセージを表示します。
error	(任意) TCAM マネージャ エラー メッセージを表示します。
move	(任意) TCAM マネージャ移行メッセージを表示します。
read	(任意) TCAM マネージャ読み込みメッセージを表示します。
write	(任意) TCAM マネージャ書き込みメッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

キーワードが指定されない場合、転送 TCAM マネージャ デバッグ メッセージがすべて表示されます。
undebug platform forw-tcam コマンドは、**no debug platform forw-tcam** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform frontend-controller

フロントエンド コントローラ アクティビティのデバッグをイネーブルにするには、**debug platform frontend-controller** 特権 EXEC 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 platform frontend-controller {all | image | led | manager | poe | register | thermal}
```

```
no debug platform frontend-controller {all | image | led | manager | poe | register | thermal}
```

シンタックスの説明

all	フロントエンド コントローラのデバッグ メッセージをすべて表示します。
image	Image Manager デバッグ メッセージを表示します
led	LED デバッグ メッセージを表示します。
manager	フロントエンド コントローラ マネージャ デバッグ メッセージを表示します。
poe	Power over Ethernet (PoE) デバッグ メッセージを表示します。
register	Register Access デバッグ メッセージを表示します。
thermal	温度デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(40)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドがサポートされているのは、Power over Ethernet スイッチだけです。

undebug platform frontend-controller コマンドは、**no debug platform frontend-controller** コマンドと同じです。

■ debug platform frontend-controller

関連コマンド

コマンド	説明
show platform frontend-controller	フロントエンドコントローラ マネージャとその従属アプリケーションのカウンタおよびステータス情報を表示します。また、フロントエンドコントローラのハードウェアおよびソフトウェア情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip arp inspection

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) インスペクション イベントをデバッグするには、**debug platform ip arp inspection** 特権 EXEC 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 platform ip arp inspection {all | error | event | packet | rpc}

no debug platform ip arp inspection {all | error | event | packet | rpc}

シンタックスの説明

all	すべてのダイナミック ARP インスペクション デバッグ メッセージを表示します。
error	ダイナミック ARP インスペクション エラー デバッグ メッセージを表示します。
event	ダイナミック ARP インスペクション イベント デバッグ メッセージを表示します。
packet	ダイナミック ARP インスペクションのパケットに関連したデバッグ メッセージを表示します。
rpc	ダイナミック ARP インスペクション Remote Procedure Call (RPC) 要求デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebbug platform ip arp inspection コマンドは、**no debug platform ip arp inspection** コマンドと同じです。

関連コマンド

コマンド	説明
show inventory	ダイナミック ARP インスペクションの設定と動作ステータスを表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip dhcp

DHCP イベントをデバッグするには、**debug platform ip dhcp** 特権 EXEC 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 platform ip dhcp [all | error | event | packet | rpc]

no debug platform ip dhcp [all | error | event | packet | rpc]

シンタックスの説明

all	(任意) DHCP デバッグ メッセージをすべて表示します。
error	(任意) DHCP エラー デバッグ メッセージを表示します。
event	(任意) DHCP イベント デバッグ メッセージを表示します。
packet	(任意) DHCP パケット関連デバッグ メッセージを表示します。
rpc	(任意) DHCP Remote Procedure Call (RPC) 要求デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip dhcp コマンドは、**no debug platform ip dhcp** コマンドと同じです。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip igmp snooping

プラットフォーム依存型インターネット グループ管理プロトコル (IGMP) スヌーピングのデバッグをイネーブルにするには、**debug platform ip igmp snooping** 特権 EXEC 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 platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

```
debug platform ip igmp snooping pak {ip-address | error | ipopt | leave | query | report | rx | svi | tx}
```

```
debug platform ip igmp snooping rpc [cfg | misc | vlan]
```

```
no debug platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

シンタックスの説明

all	すべての IGMP スヌーピング デバッグ メッセージを表示します。
di	IGMP スヌーピング宛先インデックス (di) 調整 Remote Procedure Call (RPC) デバッグ メッセージを表示します。
error	IGMP スヌーピング エラー メッセージを表示します。
event	IGMP スヌーピング イベント デバッグ メッセージを表示します。
group	IGMP スヌーピング グループ デバッグ メッセージを表示します。
mgmt	IGMP スヌーピング管理デバッグ メッセージを表示します。
pak { <i>ip-address</i> error ipopt leave query report rx svi tx }	<p>IGMP スヌーピング パケット イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> ip-address : IGMP グループの IP アドレス error : IGMP スヌーピング パケット エラー デバッグ メッセージを表示します。 ipopt : IGMP スヌーピング IP ブリッジング オプション デバッグ メッセージを表示します。 leave : IGMP スヌーピング脱退デバッグ メッセージを表示します。 query : IGMP スヌーピング クエリー デバッグ メッセージを表示します。 report : IGMP スヌーピング レポート デバッグ メッセージを表示します。 rx : IGMP スヌーピング受信パケット デバッグ メッセージを表示します。 svi : IGMP スヌーピング Switched Virtual Interface (SVI) パケット デバッグ メッセージを表示します。 tx : IGMP スヌーピング送信パケット デバッグ メッセージを表示します。
retry	IGMP スヌーピング リトライ デバッグ メッセージを表示します。

■ debug platform ip igmp snooping

rpc [cfg | misc | vlan] IGMP スヌーピング RPC イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。

- **cfg** : (任意) IGMP スヌーピング RPC デバッグ メッセージを表示します。
- **misc** : (任意) IGMP スヌーピングのその他の RPC デバッグ メッセージを表示します。
- **vlan** : (任意) IGMP スヌーピング VLAN アサート RPC デバッグ メッセージ

warn IGMP スヌーピング警告メッセージを表示します。



(注) **rpc l3mm** 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ていますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform ip igmp snooping コマンドは、**no debug platform ip igmp snooping** コマンドと同じです。

関連コマンド

コマンド	説明
debug ip igmp snooping	プラットフォーム独立 IGMP スヌーピング アクティビティに関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform ip source-guard

IP ソース ガード イベントをデバッグするには、**debug platform ip source-guard** 特権 EXEC 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 platform ip source-guard {all | error | event}
```

```
no debug platform ip source-guard {all | error | event }
```

シンタックスの説明

all	すべての IP ソース ガード プラットフォーム デバッグ メッセージを表示します。
error	IP ソース ガード プラットフォーム エラー デバッグ メッセージを表示します。
event	IP ソース ガード 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。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(50)SE	このコマンドが追加されました。

使用上のガイドライン

undebg platform ip source-guard コマンドは、**no debug platform ip source-guard** コマンドと同じです。

関連コマンド

コマンド	説明
show ip verify source	IP ソース ガードの設定を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform led

Light-Emitting Diode (LED) 動作のデバッグをイネーブルにするには、**debug platform led** 特権 EXEC 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 platform led {generic | signal}
```

```
no debug platform led {generic | signal}
```

シンタックスの説明

generic	LED 総称アクション デバッグ メッセージを表示します。
signal	LED 信号ビット マップ デバッグ メッセージを表示します。



(注)

stack 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ていますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform led コマンドは、**no debug platform led** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform matm

プラットフォームに依存する MAC（メディア アクセス制御）アドレス管理のデバッグをイネーブルにするには、**debug platform matm** 特権 EXEC 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 platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address |
  warnings}
```

```
no debug platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address |
  warnings}
```

シンタックスの説明

aging	MAC アドレス エージング デバッグ メッセージを表示します。
all	すべてのプラットフォーム MAC アドレス管理イベント デバッグ メッセージを表示します。
ec-aging	EtherChannel アドレス エージング関連デバッグ メッセージを表示します。
errors	MAC アドレス管理エラー メッセージを表示します。
learning	MAC アドレス管理アドレス学習デバッグ メッセージを表示します。
rpc	MAC アドレス管理 Remote Procedure Call (RPC; リモート プロシージャ コール) 関連デバッグ メッセージを表示します。
secure-address	MAC アドレス管理セキュア アドレス学習デバッグ メッセージを表示します。
warning	MAC アドレス管理警告メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform matm コマンドは、**no debug platform matm** コマンドと同じです。

■ debug platform matm

関連コマンド

コマンド	説明
debug matm	プラットフォーム独立 MAC アドレス管理に関する情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform messaging application

アプリケーション メッセージング アクティビティのデバッグをイネーブルにするには、**debug platform messaging application** 特権 EXEC 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 platform messaging application {all | badpak | cleanup | events | memerr |
  messages | usererr}
```

```
no debug platform messaging application {all | badpak | cleanup | events | memerr |
  messages | usererr}
```

シンタックスの説明

all	すべてのアプリケーション メッセージング デバッグ メッセージを表示します。
badpak	不良パケット デバッグ メッセージを表示します。
cleanup	クリーンアップ デバッグ メッセージを表示します。
events	イベント デバッグ メッセージを表示します。
memerr	メモリ エラー デバッグ メッセージを表示します。
messages	アプリケーション メッセージング デバッグ メッセージを表示します。
usererr	ユーザ エラー デバッグ メッセージを表示します。



(注)

stackchg 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ていますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform messaging application コマンドは、**no debug platform messaging application** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform phy

PHY (物理サブレイヤ) ドライバ情報のデバッグをイネーブルにするには、**debug platform phy** 特権 EXEC 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 platform phy {automdix | cablediag | dual-purpose | flcd {configure | ipc | iter |
  trace} | flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed
  | write | xenpak}
```

```
no debug platform phy {automdix | cablediag | dual-purpose | flcd {configure | ipc | iter
  | trace} | flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed
  | write | xenpak}
```

シンタックスの説明

automdix	PHY Automatic Medium-Dependent Interface Crossover (Auto-MDIX) デバッグ メッセージを表示します。
cablediag	PHY ケーブル診断デバッグ メッセージを表示します。
dual-purpose	PHY 兼用イベント デバッグ メッセージを表示します。
flcd {configure ipc iter trace}	PHY FLCD デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> configure : PHY 設定デバッグ メッセージを表示します。 ipc : Interprocess Communication (IPC; プロセス間通信) デバッグ メッセージを表示します。 iter : iter デバッグ メッセージを表示します。 trace : 追跡デバッグ メッセージを表示します。
flowcontrol	PHY フロー制御デバッグ メッセージを表示します。
forced	PHY 強制モード デバッグ メッセージを表示します。
init-seq	PHY 初期化シーケンス デバッグ メッセージを表示します。
link-status	PHY リンク ステータス デバッグ メッセージを表示します。
read	PHY 読み取りデバッグ メッセージを表示します。
sfp	PHY Small Form-factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュール デバッグ メッセージを表示します。
show-controller	PHY ショー コントローラ デバッグ メッセージを表示します。
speed	PHY 速度変更デバッグ メッセージを表示します。
write	PHY 書き込みデバッグ メッセージを表示します。
xenpak	PHY XENPAK デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン `undebg platform phy` コマンドは、`no debug platform phy` コマンドと同じです。

関連コマンド	コマンド	説明
	<code>show debugging</code>	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform pm

プラットフォームに依存するポート 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、**debug platform pm** 特権 EXEC 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 platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events |
idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-span |
pm-vectors [detail] | rpc [general | oper-info | state | vectors | vp-events] |
soutput-vectors | sync | vlans}
```

```
no debug platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events |
idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-span |
pm-vectors [detail] | rpc [general | oper-info | state | vectors | vp-events] |
soutput-vectors | sync | vlans}
```

シンタックスの説明

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トを表示します。
errdisable	errdisable 関連イベント デバッグ メッセージを表示します。
etherchnl	EtherChannel 関連イベント デバッグ メッセージを表示します。
exceptions	システム例外デバッグ メッセージを表示します。
hpm-events	プラットフォーム ポート マネージャ イベント デバッグ メッセージを表示します。
idb-events	Interface Descriptor Block (IDB; インターフェイス デスクリプション ブロック) 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トランスレーション イベント デバッグ メッセージを表示します。
ios-events	Cisco IOS イベント 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 マネージャ機能イベント デバッグ メッセージを表示します。
pm-events	ポート マネージャ イベント デバッグ メッセージを表示します。
pm-span	ポート マネージャ スイッチド ポート アナライザ (SPAN) 関連イベント デバッグ メッセージを表示します。
pm-vectors [detail]	ポート マネージャ ベクタ関連イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> detail : ベクタ機能詳細を表示します。
rpc [general oper-info state vectors vp-events]	RPC 関連イベント デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> general : (任意) RPC 一般イベントを表示します。 oper-info : (任意) 操作および情報関連 RPC メッセージを表示します。 state : (任意) 管理および操作関連 RPC メッセージを表示します。 vectors : (任意) ベクタ関連 RPC メッセージを表示します。 vp-events : (任意) 仮想ポート関連イベント RPC メッセージを表示します。

soutput-vectors	IDB 出力ベクタ イベント デバッグ メッセージを表示します。
sync	操作同期および VLAN ラインステート イベント デバッグ メッセージを表示します。
vlangs	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。



(注) **stack-manager** キーワードは、コマンドラインのヘルプ スtring には表示されていますが、サポートされていません。

デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **undebug platform pm** コマンドは、**no debug platform pm** コマンドと同じです。

関連コマンド	コマンド	説明
	show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform port-asic

ポート Application-Specific Integrated Circuit (ASIC; 特定用途向け集積回路) ドライバのデバッグをイネーブルにするには、**debug platform port-asic** 特権 EXEC 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 platform port-asic {**interrupt** | **periodic** | **read** | **write**}

no debug platform port-asic {**interrupt** | **periodic** | **read** | **write**}

シンタックスの説明

interrupt	ポート ASIC 割り込み関連機能デバッグ メッセージを表示します。
periodic	ポート ASIC 定期機能コール デバッグ メッセージを表示します。
read	ポート ASIC 読み取りデバッグ メッセージを表示します。
write	ポート ASIC 書き込みデバッグ メッセージを表示します。



(注)

stack キーワードは、コマンドラインのヘルプ スtring には表示されていますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform port-asic コマンドは、**no debug platform port-asic** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform port-security

プラットフォームに依存するポートセキュリティ情報のデバッグをイネーブルにするには、**debug platform port-security** 特権 EXEC 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 platform port-security {add | aging | all | delete | errors | rpc | warnings}

no debug platform port-security {add | aging | all | delete | errors | rpc | warnings}

シンタックスの説明

add	セキュア アドレス追加デバッグ メッセージを表示します。
aging	セキュア アドレス エージング デバッグ メッセージを表示します。
all	すべてのポートセキュリティ デバッグ メッセージを表示します。
delete	セキュア アドレス削除デバッグ メッセージを表示します。
errors	ポートセキュリティ エラー デバッグ メッセージを表示します。
rpc	リモートプロシージャコール (RPC) デバッグ メッセージを表示します。
warnings	警告デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform port-security コマンドは、**no debug platform port-security** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform qos-acl-tcam

QoS (Quality Of Service) およびアクセス コントロール リスト (ACL) Ternary Content Addressable Memory (TCAM) マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug platform qos-acl-tcam** 特権 EXEC 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 platform qos-acl-tcam {all | ctcam | errors | labels | mask | rpc | tcam}
```

```
no debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | rpc | tcam}
```

シンタックスの説明

all	すべての QoS および ACL TCAM (QATM) マネージャ デバッグ メッセージを表示します。
ctcam	Cisco TCAM (CTCAM) 関連イベント デバッグ メッセージを表示します。
errors	QATM エラー関連イベント デバッグ メッセージを表示します。
labels	QATM ラベル関連イベント デバッグ メッセージを表示します。
mask	QATM マスク関連イベント デバッグ メッセージを表示します。
rpc	QATM リモート プロシージャ コール (RPC) 関連イベント デバッグ メッセージを表示します。
tcam	QATM TCAM 関連イベント デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform qos-acl-tcam コマンドは、**no debug platform qos-acl-tcam** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform resource-manager

リソース マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug platform resource-manager** 特権 EXEC 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 platform resource-manager {all | dm | erd | errors | madmed | sd | stats | vld}

no debug platform resource-manager {all | dm | erd | errors | madmed | sd | stats | vld}

シンタックスの説明

all	すべてのリソース マネージャ デバッグ メッセージを表示します。
dm	宛先マップ デバッグ メッセージを表示します。
erd	等価コスト ルート記述子テーブル デバッグ メッセージを表示します。
errors	エラー デバッグ メッセージを表示します。
madmed	MAC (メディア アクセス制御) アドレス記述子テーブルおよびマルチエクspansion記述子テーブル デバッグ メッセージを表示します。
sd	ステーション記述子テーブル デバッグ メッセージを表示します。
stats	統計デバッグ メッセージを表示します。
vld	VLAN リスト記述子デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebbug platform resource-manager コマンドは、**no debug platform resource-manager** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform snmp

プラットフォームに依存する SNMP（簡易ネットワーク管理プロトコル）ソフトウェアのデバッグをイネーブルにするには、**debug platform snmp** 特権 EXEC 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 platform snmp

no debug platform snmp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform snmp コマンドは、**no debug platform snmp** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform span

プラットフォームに依存する スイッチド ポート アナライザ (SPAN) ソフトウェアのデバッグをイネーブルにするには、**debug platform span** 特権 EXEC 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 platform span

no debug platform span

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **undebug platform span** コマンドは、**no debug platform span** コマンドと同じです。

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform supervisor-asic

スーパーバイザ特定用途向け集積回路（ASIC）のデバッグをイネーブルにするには、**debug platform supervisor-asic** 特権 EXEC 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 platform supervisor-asic {all | errors | receive | send}

no debug platform supervisor-asic {all | errors | receive | send}

シンタックスの説明

all	すべてのスーパーバイザ ASIC イベント デバッグ メッセージを表示します。
errors	スーパーバイザ ASIC エラー デバッグ メッセージを表示します。
receive	スーパーバイザ ASIC 受信デバッグ メッセージを表示します。
send	スーパーバイザ ASIC 送信デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform supervisor-asic コマンドは、**no debug platform supervisor-asic** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform sw-bridge

ソフトウェアブリッジング機能のデバッグをイネーブルにするには、**debug platform sw-bridge** 特権 EXEC 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 platform sw-bridge {broadcast | control | multicast | packet | unicast}
```

```
no debug platform sw-bridge {broadcast | control | multicast | packet | unicast}
```

シンタックスの説明

broadcast	ブロードキャスト データ デバッグ メッセージを表示します。
control	プロトコル パケット デバッグ メッセージを表示します。
multicast	マルチキャスト データ デバッグ メッセージを表示します。
packet	送受信データ デバッグ メッセージを表示します。
unicast	ユニキャスト データ デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform sw-bridge コマンドは、**no debug platform sw-bridge** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform tcam

Ternary Content Addressable Memory (TCAM) アクセスおよびルックアップのデバッグをイネーブルにするには、**debug platform tcam** 特権 EXEC 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 platform tcam {log | read | search | write}
```

```
debug platform tcam log l2 {acl {input | output} | local | qos}
```

```
debug platform tcam log l3 {acl {input | output} | qos}
```

```
debug platform tcam read {reg | ssram | tcam}
```

```
debug platform tcam search
```

```
debug platform tcam write {forw-ram | reg | tcam}
```

```
no debug platform tcam {log | read | search | write}
```

```
no debug platform tcam log l2 {acl {input | output} | local | qos}
```

```
no debug platform tcam log l3 {acl {input | output} | qos}
```

```
no debug platform tcam read {reg | ssram | tcam}
```

```
no debug platform tcam search
```

```
no debug platform tcam write {forw-ram | reg | tcam}
```

シンタックスの説明

log l2 {acl {input output} local qos}	レイヤ 2 フィールド ベース CAM ルックアップ タイプ デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • acl {input output}: 入力または出力 ACL ルックアップ デバッグ メッセージを表示します。 • local: ローカル フォワーディング ルックアップ デバッグ メッセージを表示します。 • qos: 分類および QoS ルックアップ デバッグ メッセージを表示します。
l3 {acl {input output} qos}	レイヤ 3 フィールド ベース CAM ルックアップ タイプ デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • acl {input output}: 入力または出力 ACL ルックアップ デバッグ メッセージを表示します。 • qos: 分類および QoS ルックアップ デバッグ メッセージを表示します。

read {reg ssram tcam}	TCAM 読み取りデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • reg : TCAM レジスタ読み取りデバッグ メッセージを表示します。 • ssram : Synchronous Static RAM (SSRAM) 読み取りデバッグ メッセージを表示します。 • tcam : TCAM 読み取りデバッグ メッセージを表示します。
search	スーパーバイザ主導 TCAM サーチ結果デバッグ メッセージを表示します。
write {forw-ram reg tcam}	TCAM 書き込みデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <p>forw-ram : フォワーディング RAM 書き込みデバッグ メッセージを表示します。</p> <p>reg : TCAM レジスタ書き込みデバッグ メッセージを表示します。</p> <p>tcam : TCAM 書き込みデバッグ メッセージを表示します。</p>



(注)

l3 ipv6 {acl {input | output} | local | qos | secondary}、**l3 local**、および **l3 secondary** キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebg platform tcam コマンドは、**no debug platform tcam** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform udd

プラットフォームに依存する Unidirectional Link Detection (UDLD; 単方向リンク検出) ソフトウェアのデバッグをイネーブルにするには、**debug platform udd** 特権 EXEC 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 platform udd [**all** | **error** | **rpc** {**events** | **messages**}]

no debug platform udd [**all** | **error** | **rpc** {**events** | **messages**}]

シンタックスの説明

all	(任意) UDLD デバッグ メッセージをすべて表示します。
error	(任意) エラー条件デバッグ メッセージを表示します。
rpc { events messages }	(任意) UDLD リモートプロシージャコール (RPC) デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> events : UDLD RPC イベントを表示します。 messages : UDLD RPC メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebg platform udd コマンドは、**no debug platform udd** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform vlan

VLAN マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug platform vlan** 特権 EXEC 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 platform vlan {errors | mvid | rpc}
```

```
no debug platform vlan {errors | mvid | rpc}
```

シンタックスの説明

errors	VLAN エラー デバッグ メッセージを表示します。
mvid	マッピングされた VLAN ID の割り当ておよびフリー デバッグ メッセージを表示します。
rpc	リモート プロシージャ コール (RPC) デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug platform vlan コマンドは、**no debug platform vlan** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug pm

Port Manager (PM; ポート 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、**debug pm** 特権 EXEC コマンドを使用します。ポート マネージャは、すべての論理および物理インターフェイスを制御するステート マシンです。VLAN や単方向リンク検出 (UDLD) などを含むすべての機能は、ポート マネージャと連携して、スイッチに機能を提供します。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 pm {all | assert | card | etherchnl | hatable | messages | port | redundancy | registry
| sm | span | split | vlan | vp}
```

```
no debug pm {all | assert | card | etherchnl | hatable | messages | port | redundancy |
registry | sm | span | split | vlan | vp}
```

シンタックスの説明

all	すべての PM デバッグ メッセージを表示します。
assert	アサート デバッグ メッセージを表示します。
card	ラインカード関連イベント デバッグ メッセージを表示します。
etherchnl	EtherChannel 関連イベント デバッグ メッセージを表示します。
hatable	Host Access Table イベント デバッグ メッセージを表示します。
messages	PM デバッグ メッセージを表示します。
port	ポート関連イベント デバッグ メッセージを表示します。
redundancy	冗長デバッグ メッセージを表示します。
registry	PM レジストリ呼び出しデバッグ メッセージを表示します。
sm	ステート マシン関連イベント デバッグ メッセージを表示します。
span	スパニング ツリー関連イベント デバッグ メッセージを表示します。
split	スプリットプロセッサ デバッグ メッセージを表示します。
vlan	VLAN 関連イベント デバッグ メッセージを表示します。
vp	仮想ポート関連イベント デバッグ メッセージを表示します。



(注) **scp** および **pvlan** 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。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン `undebug pm` コマンドは、`no debug pm` コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug port-security

ポート セキュリティ サブシステムの割り当ておよびステータスのデバッグをイネーブ爾するには、**debug port-security** 特権 EXEC コマンドを使用します。デバッグをディセーブ爾にする場合は、このコマンドの **no** 形式を使用します。

debug port-security

no debug port-security

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デバッグはディセーブ爾です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug port-security コマンドは、**no debug port-security** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブ爾になっているデバッグ タイプに関する情報を表示します。
show port-security	インターフェイスまたはスイッチのポート セキュリティ設定を表示します。

debug qos-manager

QoS (Quality of Service) マネージャ ソフトウェアのデバッグをイネーブルにするには、**debug qos-manager** 特権 EXEC 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 qos-manager {all | event | verbose}
```

```
no debug qos-manager {all | event | verbose}
```

シンタックスの説明

all	すべての QoS マネージャ デバッグ メッセージを表示します。
event	QoS マネージャ関連イベント デバッグ メッセージを表示します。
verbose	QoS マネージャ詳細デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebbug qos-manager コマンドは、**no debug qos-manager** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug spanning-tree

スパニング ツリーのアクティビティのデバッグをイネーブルにするには、**debug spanning-tree** 特権 EXEC 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 spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events
| exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization |
uplinkfast}
```

```
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel |
events | exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization |
uplinkfast}
```

シンタックスの説明

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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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。
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 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。
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。
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、各スイッチ 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。
uplinkfast	UplinkFast イベント デバッグ メッセージを表示します。



(注)

csuf/csrt キーワードは、コマンドラインのヘルプ スtringには表示されていますが、サポートされていません。

デフォルト

デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン `undebg spanning-tree` コマンドは、`no debug spanning-tree` コマンドと同じです。

関連コマンド	コマンド	説明
	<code>show debugging</code>	イネーブルになっているデバッグ タイプに関する情報を表示します。
	<code>show spanning-tree</code>	スパンニング ツリー ステート情報を表示します。

debug spanning-tree backbonefast

スパニング ツリー BackboneFast イベントのデバッグをイネーブルにするには、**debug spanning-tree backbonefast** 特権 EXEC 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 spanning-tree backbonefast [detail | exceptions]

no debug spanning-tree backbonefast [detail | exceptions]

シンタックスの説明

detail	(任意) BackboneFast デバッグ メッセージの詳細を表示します。
exceptions	(任意) スパニング ツリー BackboneFast 例外のデバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebg spanning-tree backbonefast コマンドは、**no debug spanning-tree backbonefast** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree bpdu

送受信されたスパニング ツリー ブリッジ プロトコル データ ユニット (BPDU) のデバッグをイネーブルにするには、**debug spanning-tree bpdu** 特権 EXEC 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 spanning-tree bpdu [receive | transmit]

no debug spanning-tree bpdu [receive | transmit]

シンタックスの説明

receive	(任意) 受信 BPDU 用非最適化パスのデバッグ メッセージを表示します。
transmit	(任意) 送信された BPDU デバッグ メッセージについて、最適化されないパスを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebg spanning-tree bpdu コマンドは、**no debug spanning-tree bpdu** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree bpdu-opt

最適化されたスパニング ツリー ブリッジ プロトコル データ ユニット (BPDU) 処理のデバッグをイネーブルにするには、**debug spanning-tree bpdu-opt** 特権 EXEC 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 spanning-tree bpdu-opt [detail | packet]

no debug spanning-tree bpdu-opt [detail | packet]

シンタックスの説明

detail	(任意) 最適化された BPDU 処理デバッグ メッセージの詳細を表示します。
packet	(任意) パケット レベルの最適化された BPDU 処理デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug spanning-tree bpdu-opt コマンドは、**no debug spanning-tree bpdu-opt** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show spanning-tree	スパニング ツリー ステート情報を表示します。

debug spanning-tree mstp

Multiple Spanning-Tree Protocol (MSTP) ソフトウェアのデバッグをイネーブルにするには、**debug spanning-tree mstp** 特権 EXEC 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 spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init |
migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

```
no debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init |
migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

シンタックスの説明

all	デバッグ メッセージをすべてイネーブルにします。
boundary	次に示す境界上でのフラグ変更をデバッグします。 <ul style="list-style-type: none"> Multiple Spanning-Tree (MST) リージョンと、Rapid Spanning-Tree Protocol (RSTP) が稼動する単一のスパニング ツリー リージョンとの境界 MST リージョンと、802.1D が稼動する単一のスパニング ツリー リージョンとの境界 MST リージョンと、設定が異なる別の MST リージョンとの境界
bpdu-rx	受信した MST ブリッジプロトコルデータ ユニット (BPDU) をデバッグします。
bpdu-tx	送信された MST BPDU をデバッグします。
errors	MSTP エラーをデバッグします。
flush	ポート フラッシュ メカニズムをデバッグします。
init	MSTP データ構造の初期化をデバッグします。
migration	プロトコル移行ステート マシンをデバッグします。
pm	MSTP ポート マネージャ イベントをデバッグします。
proposals	指定スイッチとルート スイッチ間のハンドシェイク メッセージをデバッグします。
region	Switch Processor (SP; スイッチ プロセッサ) と Route Processor (RP; ルート プロセッサ) 間のリージョン同期をデバッグします。
roles	MSTP のロールをデバッグします。
sanity_check	受信した BPDU の正常性確認メッセージをデバッグします。
sync	ポート同期イベントをデバッグします。
tc	トポロジ変更通知イベントをデバッグします。
timers	開始、停止、および期限切れイベントの MSTP タイマーをデバッグします。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

■ debug spanning-tree mstp

使用上のガイドライン `undebug spanning-tree mstp` コマンドは、`no debug spanning-tree mstp` コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	イネーブルになっているデバッグ タイプに関する情報を表示します。
<code>show spanning-tree</code>	スパニング ツリー ステート情報を表示します。

debug spanning-tree switch

スパニング ツリー プロトコル (STP) ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール間のソフトウェア インターフェイスのデバッグをイネーブルにするには、**debug spanning-tree switch** 特権 EXEC 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 spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors | interrupt | process} | state | tx [decode] | uplinkfast}
```

```
no debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors | interrupt | process} | state | tx [decode] | uplinkfast}
```

シンタックスの説明

all	スパニング ツリー スイッチのデバッグ メッセージをすべて表示します。
errors	スパニング ツリー ソフトウェア モジュールとポート マネージャ ソフトウェア モジュール間のインターフェイスに関するデバッグ メッセージを表示します。
flush	シム フラッシュ動作に関するデバッグ メッセージを表示します。
general	一般イベント デバッグ メッセージを表示します。
helper	スパニング ツリー ヘルパー タスク デバッグ メッセージを表示します。ヘルパー タスクは大容量スパニング ツリー更新を処理します。
pm	ポート マネージャ イベント デバッグ メッセージを表示します。
rx	受信したブリッジプロトコル データ ユニット (BPDU) 処理のデバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • decode : デコード済み受信パケットを表示します。 • errors : 受信エラー デバッグ メッセージを表示します。 • interrupt : Interrupt Service Request (ISR) デバッグ メッセージを表示します。 • process : 処理受信 BPDU デバッグ メッセージを表示します。
state	スパニング ツリー ポート ステート変更デバッグ メッセージを表示します。
tx [decode]	送信された BPDU 処理デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • decode : (任意) デコードされた送信パケットを表示します。
uplinkfast	UplinkFast パケット送信デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

■ debug spanning-tree switch

使用上のガイドライン `undebug spanning-tree switch` コマンドは、`no debug spanning-tree switch` コマンドと同じです。

関連コマンド

コマンド	説明
<code>show debugging</code>	イネーブルになっているデバッグ タイプに関する情報を表示します。
<code>show spanning-tree</code>	スパニング ツリー ステート情報を表示します。

debug spanning-tree uplinkfast

スパニング ツリー UplinkFast イベントのデバッグをイネーブルにするには、**debug spanning-tree uplinkfast** 特権 EXEC 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 spanning-tree uplinkfast [exceptions]

no debug spanning-tree uplinkfast [exceptions]

シンタックスの説明	exceptions (任意) スパニング ツリー UplinkFast 例外のデバッグ メッセージを表示します。
-----------	--

デフォルト	デバッグはディセーブルです。
-------	----------------

コマンド モード	特権 EXEC
----------	---------

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン	undebug spanning-tree uplinkfast コマンドは、 no debug spanning-tree uplinkfast コマンドと同じです。
------------	--

関連コマンド	コマンド	説明
	show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
	show spanning-tree	スパニング ツリー ステート情報を表示します。

debug sw-vlan

VLAN マネージャのアクティビティのデバッグをイネーブルにするには、**debug sw-vlan** 特権 EXEC 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 sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management |
mapping | notification | packets | redundancy | registries | vtp}
```

```
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management |
mapping | notification | packets | redundancy | registries | vtp}
```

シンタックスの説明

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 {bootup cli}	config-vlan デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> bootup : スイッチがブートアップするときにメッセージを表示します。 cli : CLI (コマンドライン インターフェイス) が config-vlan 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	debug sw-vlan ifs コマンドを参照してください。
management	内部 VLAN の VLAN マネージャ管理のデバッグ メッセージを表示します。
mapping	VLAN マッピングのデバッグ メッセージを表示します。
notification	debug sw-vlan notification コマンド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	debug sw-vlan vtp コマンドを参照してください。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug sw-vlan コマンドは、**no debug sw-vlan** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグタイプに関する情報を表示します。
show vlan	管理ドメインに設定されたすべての VLAN または特定の VLAN (VLAN 名または ID を指定した場合) のパラメータを表示します。
show vtp	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します。

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、**debug sw-vlan ifs** 特権 EXEC 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 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}
```

シンタックスの説明

open {read write}	VLAN マネージャ IFS ファイルオープン操作デバッグ メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> 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。 write : VLAN マネージャ IFS ファイル書き込み操作デバッグ メッセージを表示します。
read {1 2 3 4}	指定されたエラー リスト (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。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

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。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグタイプに関する情報を表示します。
show vlan	管理ドメインに設定されたすべての VLAN または特定の VLAN (VLAN 名または ID を指定した場合) のパラメータを表示します。

debug sw-vlan notification

ISL（スイッチ間リンク）VLAN ID のアクティブ化および非アクティブ化のデバッグをイネーブルにするには、**debug sw-vlan notification** 特権 EXEC 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 sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange |
linkchange | modechange | pruningcfgchange | statechange}
```

```
no debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange |
linkchange | modechange | pruningcfgchange | statechange}
```

シンタックスの説明

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。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug sw-vlan notification コマンドは、**no debug sw-vlan notification** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show vlan	管理ドメインに設定されたすべての VLAN または特定の VLAN (VLAN 名または ID を指定した場合) のパラメータを表示します。

debug sw-vlan vtp

VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) コードのデバッグをイネーブルにするには、**debug sw-vlan vtp** 特権 EXEC 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 sw-vlan vtp {events | packets | pruning [packets | xmit] | redundancy | xmit}

no debug sw-vlan vtp {events | packets | pruning | redundancy | xmit}

シンタックスの説明

events	汎用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詳細な VTP メッセージを表示します。
packets	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 [packets xmit]	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。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • packets : (任意) 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 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 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。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug sw-vlan vtp コマンドは、**no debug sw-vlan vtp** コマンドと同じです。

pruning キーワードのあとにパラメータを指定しない場合は、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。

■ debug sw-vlan vtp

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show vtp	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します。

debug udld

単方向リンク検出 (UDLD) 機能のデバッグをイネーブルにするには、**debug udld** 特権 EXEC コマンドを使用します。UDLD 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 udld {events | packets | registries}
```

```
no debug udld {events | packets | registries}
```

シンタックスの説明	events	UDLD プロセス イベントが発生したときのデバッグ メッセージを表示します。
	packets	UDLD プロセスがパケット キューからパケットを受信し、UDLD プロトコル コードの要求に応答してそれらを送信するときに、このプロセスのデバッグ メッセージを表示します。
	registries	UDLD プロセスが UDLD プロセスに依存するモジュールおよびその他のフィチャ モジュールからのレジストリ コールを処理するときに、このプロセスのデバッグ メッセージを表示します。

デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン **undebg udld** コマンドは、**no debug udld** コマンドと同じです。
debug udld events を入力すると、次に示すデバッグ メッセージが表示されます。

- 一般的な UDLD プログラム論理フロー
- ステート マシンのステート変更
- errdisable ステートの設定および消去のプログラム アクション
- 近接キャッシュの追加および削除
- コンフィギュレーション コマンドの処理
- リンクアップおよびリンクダウン通知処理

debug udld packets を入力すると、次に示すデバッグ メッセージが表示されます。

- 着信パケット受信時の一般的なパケット処理プログラム フロー
- 受信したパケットをパケット受信コードで調べるときの、各パケットの内容の識別情報 (Type Length Version [TLV] など)
- パケット送信の試行内容およびその成果

debug udld registries を入力すると、次に示すカテゴリのデバッグ メッセージが表示されます。

- サブブロックの作成

■ debug udd

- ファイバポート ステータスの変更
- ポート マネージャ ソフトウェアからのステート変更通知情報
- MAC (メディア アクセス制御) アドレス レジストリ コール

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show udd	すべてのポートまたは指定されたポートの UDD 管理上および運用上のステータスを表示します。

debug vqpc

VLAN Query Protocol (VQP) クライアントのデバッグをイネーブルにするには、**debug vqpc** 特権 EXEC 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 vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

シンタックスの説明

all	(任意) VQP クライアント デバッグ メッセージをすべて表示します。
cli	(任意) VQP クライアント CLI (コマンドライン インターフェイス) デバッグ メッセージを表示します。
events	(任意) VQP クライアント イベント デバッグ メッセージを表示します。
learn	(任意) VQP クライアント アドレス学習デバッグ メッセージを表示します。
packet	(任意) VQP クライアント パケット情報デバッグ メッセージを表示します。

デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

undebug vqpc コマンドは、**no debug vqpc** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

■ debug vqpc



APPENDIX **C**

Catalyst 2960 スイッチ show platform コマンド

この付録では、Catalyst 2960 スイッチで使用するために作成または変更された **show platform** 特権 EXEC コマンドについて説明します。これらのコマンドは、インターネットワーキングの問題の診断および解決に役立つ情報を示します。使用する場合には、必ずシスコのテクニカル サポート担当者の指示に従ってください。

show platform acl

プラットフォームに依存する Access Control List (ACL; アクセス コントロール リスト) マネージャ情報を表示するには、**show platform acl** 特権 EXEC コマンドを使用します。

```
show platform acl {interface interface-id | label label-number [detail] | statistics asic-number
| usage asic-number [summary] | vlan vlan-id} [| {begin | exclude | include} expression]
```

シンタックスの説明

interface interface-id	指定されたインターフェイスについてインターフェイス単位の ACL マネージャ情報を表示します。このインターフェイスは物理インターフェイスまたは Virtual LAN (VLAN; 仮想 LAN) になることができます。
label label-number [detail]	ラベル単位の ACL マネージャ情報を表示します。指定できる <i>label-number</i> の範囲は 0 ~ 255 です。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> detail : (任意) 詳細 ACL マネージャ ラベル情報を表示します。
statistics asic-number	ASIC (特定用途向け集積回路) 単位の ACL マネージャ情報を表示します。 <i>asic-number</i> は、ポート ASIC 番号で、0 または 1 です。
usage asic-number [summary]	ASIC 単位の ACL 使用状況情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> summary : (任意) 使用状況情報の概要を表示します。
vlan vlan-id	VLAN 単位の ACL マネージャ情報を表示します。指定できる <i>vlan-id</i> の範囲は 1 ~ 4094 です。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform backup interface

Flex Link 設定で使用されるプラットフォーム依存型バックアップ情報を表示するには、**show platform backup interface** 特権 EXEC コマンドを使用します。

```
show platform backup interface [interface-id | dummyQ] [| {begin | exclude | include}
expression]
```

シンタックスの説明

<i>interface-id</i>	(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に対するバックアップ情報を表示します。インターフェイスは、物理インターフェイスでもポート チャネルでもかまいません。
dummyQ	(任意) ダミー キュー情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform etherchannel

プラットフォームに依存する EtherChannel 情報を表示するには、**show platform etherchannel** 特権 EXEC コマンドを使用します。

```
show platform etherchannel {flags | time-stamps} [| {begin | exclude | include}
expression]
```

シンタックスの説明

flags	EtherChannel ポート フラグを表示します。
time-stamps	EtherChannel タイム スタンプを表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform forward

指定されたパラメータと一致したフレームがハードウェアで転送される方法を指定するには、インターフェイスに対して **show platform forward** 特権 EXEC コマンドを使用します。

```
show platform forward interface-id [vlan vlan-id] src-mac dst-mac [l3protocol-id] [sap |
snap] [cos cos] [ip src-ip dst-ip [frag field] [dscp dscp] {l4protocol-id | icmp icmp-type
icmp-code | igmp igmp-version igmp-type | sctp src-port dst-port | tcp src-port dst-port
flags | udp src-port dst-port}] [ {begin | exclude | include} expression]
```

シンタックスの説明

<i>interface-id</i>	パケットがスイッチに着信するポートとなる入力物理インターフェイス (タイプ、ポート番号を含む)。
<i>vlan vlan-id</i>	(任意) 入力 VLAN ID。指定できる範囲は 1 ~ 4094 です。このパラメータに値を指定せず、入力インターフェイスがルーテッドポートでない場合は、デフォルト値が 1 になります。
<i>src-mac</i>	48 ビット送信元 MAC (メディア アクセス制御) アドレス。
<i>dst-mac</i>	48 ビット宛先 MAC アドレス。
<i>l3protocol-id</i>	(任意) パケットで使用されるレイヤ 3 プロトコル。指定できる範囲は 0 ~ 65535 です。
<i>sap</i>	(任意) Service Access Point (SAP; サービス アクセスポイント) カプセル化タイプ。
<i>snap</i>	(任意) Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル) カプセル化タイプ。
<i>cos cos</i>	(任意) フレームの Class of Service (CoS; サービス クラス) 値。指定できる範囲は 0 ~ 7 です。
<i>ip src-ip dst-ip</i>	(任意、ただし IP パケットには必要) ドット付き 10 進表記の送信元および宛先 IP アドレス。
<i>frag field</i>	(任意) フラグメント IP パケットの IP フラグメントフィールド。指定できる範囲は 0 ~ 65535 です。
<i>dscp dscp</i>	(任意) IP ヘッダーの Differentiated Service Code Point (DSCP) フィールド。指定できる範囲は 0 ~ 63 です。
<i>l4protocol-id</i>	IP ヘッダーのレイヤ 4 プロトコル フィールドの数値。指定できる範囲は 0 ~ 255 です。たとえば、47 は Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) であり、89 は OSPF (Open Shortest Path First) です。プロトコルが TCP、User Datagram Protocol (UDP)、Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル)、または Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) である場合、数値の代わりに適切なキーワードを使用する必要があります。
<i>icmp icmp-type icmp-code</i>	ICMP パラメータ。指定できる <i>icmp-type</i> および <i>icmp-code</i> の範囲は 0 ~ 255 です。
<i>igmp igmp-version igmp-type</i>	IGMP パラメータ。指定できる <i>igmp-version</i> の範囲は 1 ~ 15 であり、指定できる <i>igmp-type</i> の範囲は 0 ~ 15 です。
<i>sctp src-port dst-port</i>	Stream Control Transmission Protocol (SCTP) パラメータ。SCTP 送信元および宛先ポートに指定できる範囲は 0 ~ 65535 です。
<i>tcp src-port dst-port flags</i>	TCP パラメータ: TCP 送信元ポート、宛先ポート、およびヘッダー内の TCP フラグ バイトの数値。指定できる <i>src-port</i> および <i>dst-port</i> の範囲は 0 ~ 65535 です。指定できるフラグの範囲は 0 ~ 1024 です。

show platform forward

udp <i>src-port dst-port</i>	UDP パラメータ。指定できる <i>src-port</i> および <i>dst-port</i> の範囲は 0 ~ 65535 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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

show platform forward コマンドの出力表示およびその意味の例については、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「Troubleshooting」の章を参照してください。

show platform ip igmp snooping

プラットフォーム依存型インターネットグループ管理プロトコル (IGMP) スヌーピング情報を表示するには、**show platform ip igmp snooping** 特権 EXEC コマンドを使用します。

```
show platform ip igmp snooping {all | control [di] | counters | flood [vlan vlan-id] | group
ip-address | hardware | retry [count | local [count] | remote [count]]} [| {begin |
exclude | include} expression]
```

シンタックスの説明

all	すべての IGMP スヌーピング プラットフォーム IP マルチキャスト情報を表示します。
control [di]	IGMP スヌーピング コントロール エントリを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> di : (任意) IGMP スヌーピング コントロール宛先索引エントリを表示します。
counters	IGMP スヌーピング カウンタを表示します。
flood [vlan vlan-id]	IGMP スヌーピング フラッディング情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> vlan vlan-id : (任意) 指定された VLAN のフラッディング情報を表示します。指定できる範囲は 1 ~ 4094 です。
group ip-address	IGMP スヌーピング マルチキャスト グループ情報を表示します。ここで、 <i>ip-address</i> はグループの IP アドレスです。
hardware	ハードウェアにロードされた IGMP スヌーピング情報を表示します。
retry [count local [count]]	IGMP スヌーピング再試行情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> count : (任意) 再試行回数だけを表示します。 local : (任意) ローカル再試行エントリを表示します。
remote [count]	リモート エントリを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> count : (任意) リモート カウントだけを表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

■ show platform ip igmp snooping

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform layer4op

プラットフォームに依存するレイヤ 4 演算子情報を表示するには、**show platform layer4op** 特権 EXEC コマンドを使用します。

```
show platform layer4op {acl | pacl [port-asic] | qos [port-asic]} {and-or | map | or-and | vcu}
[ | {begin | exclude | include} expression]
```

シンタックスの説明

acl	アクセス コントロール リスト (ACL) レイヤ 4 オペレータ情報を表示します。
pacl [port-asic]	ポート ACL レイヤ 4 オペレータ情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <i>port-asic</i> : (任意) ポート ASIC (特定用途向け集積回路) 番号を表示します。
qos [port-asic]	QoS (Quality of Service) レイヤ 4 オペレータ情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <i>port-asic</i> : (任意) QoS ポート ASIC 番号を表示します。
and-or	AND-OR レジスタ情報を表示します。
map	選択マップ情報を表示します。
or-and	OR-AND レジスタ情報を表示します。
vcu	Value Compare Unit (VCU) レジスタ情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform mac-address-table

プラットフォーム依存型 MAC（メディア アクセス制御）アドレス テーブル情報を表示するには、**show platform mac-address-table** 特権 EXEC コマンドを使用します。

```
show platform mac-address-table [aging-array | hash-table | mac-address mac-address]
[vlan vlan-id] [| {begin | exclude | include} expression]
```

シンタックスの説明

aging-array	(任意) MAC アドレス テーブル エージング アレイを表示します。
hash-table	(任意) MAC アドレス テーブル ハッシュ テーブルを表示します。
mac-address mac-address	(任意) MAC アドレス テーブル MAC アドレス情報を表示します。ここで、 <i>mac-address</i> は 48 ビット ハードウェア アドレスです。
vlan vlan-id	(任意) 指定された VLAN の情報を表示します。指定できる範囲は 1 ~ 4094 です。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform messaging

プラットフォームに依存するアプリケーションおよびパフォーマンス メッセージ情報を表示するには、**show platform messaging** 特権 EXEC コマンドを使用します。

```
show platform messaging {application [incoming | outgoing | summary] | hiperf
[class-number]} [| {begin | exclude | include} expression]
```

シンタックスの説明

application [incoming outgoing summary]	アプリケーション メッセージ情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> incoming : (任意) 着信アプリケーション メッセージング要求に関する情報だけを表示します。 outgoing : (任意) 発信アプリケーション メッセージング要求に関する情報だけを表示します。 summary : (任意) アプリケーション メッセージング要求すべてに関するサマリー情報を表示します。
hiperf [class-number]	発信するハイパフォーマンス メッセージ情報を表示します。特定のクラス番号のハイパフォーマンス メッセージについての情報を表示するには、 <i>class-number</i> オプションを指定します。指定できる範囲は 0 ~ 36 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform monitor

プラットフォームに依存する Switched Port Analyzer (SPAN; スイッチドポートアナライザ) 情報を表示するには、**show platform monitor** 特権 EXEC コマンドを使用します。

```
show platform monitor [session session-number] [| {begin | exclude | include} expression]
```

シンタックスの説明

session	(任意) 指定された SPAN セッションの SPAN 情報を表示します。指定できる範囲は 1 ~ 66 です。
session-number	(任意) 指定された SPAN セッションの SPAN 情報を表示します。指定できる範囲は 1 ~ 66 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
expression	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカルサポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform mvr table

プラットフォーム依存型 Multicast VLAN Registration (MVR) Multi-Expansion Descriptor (MED) グループ マッピング テーブルを表示するには、**show platform mvr table** 特権 EXEC コマンドを使用します。

```
show platform mvr table [| {begin | exclude | include} expression]
```

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform pm

プラットフォームに依存するポート マネージャ情報を表示するには、**show platform pm** 特権 EXEC コマンドを使用します。

```
show platform pm {counters | group-masks | idbs {active-idbs | deleted-idbs} |
  if-numbers | link-status | platform-block | port-info interface-id | vlan {info |
  line-state}
  [| {begin | exclude | include} expression]
```

シンタックスの説明

counters	モジュール カウンタ情報を表示します。
group-masks	EtherChannel グループ マスク情報を表示します。
idbs {active-idbs deleted-idbs}	Interface Data Block (IDB) 情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> active-idbs : アクティブ IDB 情報を表示します。 deleted-idbs : 削除または漏洩された IDB 情報を表示します。
if-numbers	インターフェイス番号情報を表示します。
link-status	ローカル ポート リンク ステータス情報を表示します。
platform-block	プラットフォーム ポート ブロック情報を表示します。
port-info interface-id	指定されたインターフェイスのポート管理および動作フィールドを表示します。
vlan {info line-state}	プラットフォーム VLAN 情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> info : アクティブ VLAN の情報を表示します。 line-state : ラインステート情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注)

stack-view 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ていますが、サポートされていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform port-asic

プラットフォーム依存型ポート ASIC（特定用途向け集積回路）レジスタ情報を表示するには、**show platform port-asic** 特権 EXEC コマンドを使用します。

```
show platform port-asic {cpu-queue-map-table [asic number | port number [asic number]] |
  dest-map index number |
  etherchannel-info [asic number | port number [asic number]] |
  exception [asic number | port number [asic number]] |
  global-status [asic number | port number [asic number]] |
  learning [asic number | port number [asic number]] |
  mac-info [asic number | port number [asic number]] |
  mvid [asic number] |
  packet-info-ram [asic number | index number [asic number]] |
  port-info [asic number | port number [asic number]] |
  prog-parser [asic number | port number [asic number]] |
  receive {buffer-queue | port-fifo | supervisor-sram} [asic number | port number [asic
  number]] |
  span [vlan-id [asic number] | [asic number]
  stats {drop | enqueue | miscellaneous | supervisor} [asic number | port number [asic
  number]] |
  transmit {port-fifo | queue | supervisor-sram} [asic number | port number [asic number]]
  vct [asic number | port number [asic number]]
  version}
  [ | {begin | exclude | include} expression]
```

シンタックスの説明

cpu-queue-map-table [asic number port number [asic number]]	CPU キュー マップ テーブル エントリを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。
dest-map index number	指定された索引の宛先マップ情報を表示します。指定できる範囲は 0 ~ 65535 です。
etherchannel-info [asic number port number [asic number]]	EtherChannel 情報レジスタの内容を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
exception [asic number port number [asic number]]	例外索引レジスタ情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。

global-status [<i>asic number</i> <i>port number</i> [<i>asic number</i>]]	<p>グローバルおよび中断ステータスを表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
learning [<i>asic number</i> <i>port number</i> [<i>asic number</i>]]	<p>学習キャッシュ内のエントリを表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
mac-info [<i>asic number</i> <i>port number</i> [<i>asic number</i>]]	<p>MAC (メディア アクセス制御) 情報レジスタの内容を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
mvid [<i>asic number</i>]	<p>マッピングされた VLAN ID テーブルを表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。
packet-info-ram [<i>asic number</i> <i>index number</i> [<i>asic number</i>]]	<p>パケット情報 RAM を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • index number : (任意) 指定されたパケット RAM 索引番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 63 です。
port-info [<i>asic number</i> <i>port number</i> [<i>asic number</i>]]	<p>ポート情報レジスタ値を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
prog-parser [<i>asic number</i> <i>port number</i> [<i>asic number</i>]]	<p>プログラマブル パーサ テーブルを表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。

receive { buffer-queue port-fifo supervisor-sram } [asic number port number [asic number]]	<p>受信情報を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • buffer-queue : バッファ キュー情報を表示します。 • port-fifo : ポート First-In, First-Out (FIFO; ファーストインファーストアウト) 情報を表示します。 • supervisor-sram : スーパーバイザ SRAM 情報を表示します。 • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
span [vlan-id asic number]	<p>スイッチド ポート アナライザ (SPAN) 関連情報を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • vlan-id : (任意) 指定された VLAN の情報を表示します。指定できる範囲は 0 ~ 1023 です。 • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。
stats { drop enqueue miscellaneous supervisor } [asic number port number [asic number]]	<p>ポート ASIC の未処理の統計を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • drop : 廃棄統計情報を表示します。 • enqueue : エンキュー統計情報を表示します。 • miscellaneous : 各種情報を表示します。 • supervisor : スーパーバイザ統計情報を表示します。 • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
transmit { port-fifo queue supervisor-sram } [asic number port number [asic number]]	<p>送信情報を表示します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • port-fifo : ポート FIFO 情報レジスタの内容を表示します。 • queue : キュー情報レジスタの内容を表示します。 • supervisor-sram : スーパーバイザ SRAM 情報を表示します。 • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。0 はスーパーバイザで、1 ~ 25 はポートを示します。

vct [asic number port number [asic number]]	指定された ASIC または指定されたポートおよび ASIC の VLAN 圧縮テーブル エントリを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • asic number : (任意) 指定された ASIC の情報を表示します。指定できる範囲は 0 ~ 1 です。 • port number : (任意) 指定されたポート番号と ASIC 番号の情報を表示します。指定できる範囲は 0 ~ 27 です。ここで 0 はスーパーバイザであり、1 ~ 25 はポートです。
version	ポート ASIC のバージョンおよびデバイス タイプ情報を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注)

stack {**control** | **dest-map** | **learning** | **messages** | **mvid** | **prog-parser** | **span** | **stats** [**asic number** | **port number** [**asic number**]} キーワードは、コマンドラインのヘルプ スtringには表示されていますが、サポートされていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform port-security

プラットフォームに依存するポートセキュリティ情報を表示するには、**show platform port-security** 特権 EXEC コマンドを使用します。

show platform port-security [| {**begin** | **exclude** | **include**} *expression*]

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform qos

プラットフォーム依存型 QoS (Quality of Service) 情報を表示するには、**show platform qos** 特権 EXEC コマンドを使用します。

```
show platform qos {label asic number | policer {parameters asic number |
port alloc number asic number}} [| {begin | exclude | include} expression]
```

シンタックスの説明

label asic number	指定された ASIC (特定用途向け集積回路) の QoS ラベルマップを表示します。 (任意) asic number に指定できる範囲は 0 ~ 1 です。
policer {parameters asic number port alloc number asic number}	ポリサー情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • parameters asic number : 指定された ASIC のパラメータ情報を表示します。指定できる範囲は 0 ~ 1 です。 • port alloc number asic number : 指定されたポートおよび ASIC のポート割り当て情報を表示します。指定できるポート割り当て範囲は 0 ~ 25 です。指定できる ASIC 範囲は 0 ~ 1 です。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform resource-manager

プラットフォームに依存するリソース マネージャ情報を表示するには、**show platform resource-manager** 特権 EXEC コマンドを使用します。

```
show platform resource-manager {dm [index number] | erd [index number] |
  mad [index number] | med [index number] | mod | msm {hash-table [vlan vlan-id] |
  mac-address mac-address [vlan vlan-id]} | sd [index number] |
  vld [index number]} [ | {begin | exclude | include} expression]
```

シンタックスの説明

dm [index number]	宛先マップを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> index number : (任意) 指定された索引を表示します。指定できる範囲は 0 ~ 65535 です。
erd [index number]	指定された索引の等価コスト ルート記述子テーブルを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> index number : (任意) 指定された索引を表示します。指定できる範囲は 0 ~ 65535 です。
mad [index number]	指定されたインデックスの MAC (メディア アクセス制御) アドレス記述子テーブルを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> index number : (任意) 指定された索引を表示します。指定できる範囲は 0 ~ 65535 です。
med [index number]	指定された索引のマルチエクスペンション記述子テーブルを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> index number : (任意) 指定された索引を表示します。指定できる範囲は 0 ~ 65535 です。
mod	リソースマネージャ モジュール情報を表示します。
msm {hash-table [vlan vlan-id] mac-address mac-address [vlan vlan-id]}	MAC アドレス記述子テーブルおよびステーション記述子テーブル情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> hash-table [vlan vlan-id] : すべての VLAN または指定された VLAN のハッシュ テーブルを表示します。指定できる範囲は 1 ~ 4094 です。 mac-address mac-address [vlan vlan-id] : すべての VLAN または指定された VLAN に対して 48 ビットのハードウェア アドレスで表された MAC アドレスの MAC アドレス記述子テーブルを表示します。指定できる範囲は 1 ~ 4094 です。
sd [index number]	指定された索引のステーション記述子テーブルを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> index number : (任意) 指定された索引を表示します。指定できる範囲は 0 ~ 65535 です。
vld [index number]	指定されたインデックスの VLAN リスト記述子テーブルを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> index number : (任意) 指定された索引を表示します。指定できる範囲は 0 ~ 65535 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。

include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform snmp counters

プラットフォームに依存するの SNMP (簡易ネットワーク管理プロトコル) カウンタ情報を表示するには、**show platform snmp counters** 特権 EXEC コマンドを使用します。

```
show platform snmp counters [ | {begin | exclude | include} expression]
```

シンタックスの説明

begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform spanning-tree

プラットフォーム依存型スパンニングツリー情報を表示するには、**show platform spanning-tree** 特権 EXEC コマンドを使用します。

```
show platform spanning-tree synchronization [detail | vlan vlan-id] [ | {begin | exclude | include} expression]
```

シンタックスの説明

synchronization [detail vlan <i>vlan-id</i>]	スパンニングツリー ステート同期情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none">• detail : (任意) スパンニングツリー情報の詳細を表示します。• vlan <i>vlan-id</i> : (任意) 指定された VLAN の VLAN スイッチ スパンニングツリー情報を表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform stp-instance

プラットフォーム依存型スパンニングツリー インスタンス情報を表示するには、**show platform stp-instance** 特権 EXEC コマンドを使用します。

```
show platform stp-instance vlan-id [ | {begin | exclude | include} expression]
```

シンタックスの説明

<i>vlan-id</i>	指定された VLAN のスパンニングツリー インスタンス情報を表示します。指定できる範囲は 1 ~ 4094 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

stack manager

sshow platform tcam

buffer	ポート リンク イベントと同期ステート イベントを表示します。
history	ポート履歴を表示します。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

プラットフォームに依存する Ternary Content Addressable Memory (TCAM) ドライバ情報を表示するには、**show platform tcam** 特権 EXEC コマンドを使用します。

```
show platform tcam {handle number | log-results | table {acl | all | local | mac-address | qos
| station | vlan-list} | usage} [asic number [detail [invalid]] | [index number [detail
[invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table acl [asic number [detail [invalid]] | [index number [detail
[invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table all [asic number [detail [invalid]] | [index number [detail
[invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table local [asic number [detail [invalid]] | [index number [detail
[invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table mac-address [asic number [detail [invalid]] | [index number
[detail [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num
number [detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table qos [asic number [detail [invalid]] | [index number [detail
[invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table station [asic number [detail [invalid]] | [index number [detail
[invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

```
show platform tcam table vlan-list [ [asic number [detail [invalid]] | [index number [detail
[invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number
[detail [invalid]] | invalid]] [ | {begin | exclude | include} expression]
```

シンタックスの説明

handle number	TCAM ハンドルを表示します。指定できる範囲は 0 ~ 4294967295 です。
log-results	TCAM ログ結果を表示します。

table { acl all local mac-address qos station vlan-list }	ルックアップおよび転送テーブル情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • acl : アクセス コントロール リスト (ACL) テーブルを表示します。 • all : すべての TCAM テーブルを表示します。 • local : ローカル テーブルを表示します。 • mac-address : MAC (メディア アクセス制御) アドレス テーブルを表示します。 • qos : QoS テーブルを表示します。 • station : ステーション テーブルを表示します。 • vlan-list : VLAN リスト テーブルを表示します。
usage	CAM (連想メモリ) および転送テーブル使用状況を表示します。
[[asic number [detail [invalid]] [index number [detail [invalid]] invalid num number [detail [invalid]] invalid] [invalid] [num number [detail [invalid]] invalid]]	情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • asic number : 指定された ASIC デバイス ID の情報を表示します。指定できる範囲は 0 ~ 15 です。 • detail [invalid] : (任意) 有効または無効詳細を表示します。 • index number : (任意) 指定された TCAM テーブル索引の情報を表示します。指定できる範囲は 0 ~ 32768 です。 • num number : (任意) 指定された TCAM テーブル番号の情報を表示します。指定できる範囲は 0 ~ 32768 です。
begin	(任意) <i>expression</i> と一致する行から表示を開始します。
exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。



(注)

ipv6、**equal-cost-route**、**multicast-expansion**、**secondary**、および **usage** キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。

コマンドモード 特権 EXEC

コマンドの履歴	リリース	変更内容
	12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。

show platform vlan

プラットフォームに依存する VLAN 情報を表示するには、**show platform vlan** 特権 EXEC コマンドを使用します。

```
show platform vlan {misc | mvid | prune | refcount | rpc {receive | transmit}} [| {begin |
exclude | include} expression]
```

シンタックスの説明

misc	各種 VLAN モジュール情報を表示します。
mvid	Mapped VLAN ID (MVID) 割り当て情報を表示します。
prune	プラットフォームで維持されるブルーニング データベースを表示します。
refcount	VLAN ロック モジュールについてのリファレンス カウントを表示します。
rpc {receive transmit}	Remote Procedure Call (RPC; リモート プロシージャ コール) メッセージを表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • receive : 受信した情報を表示します。 • transmit : 送信した情報を表示します。
 begin	(任意) <i>expression</i> と一致する行から表示を開始します。
 exclude	(任意) <i>expression</i> と一致する行を表示から除外します。
 include	(任意) 指定された <i>expression</i> と一致する行を表示に含めます。
<i>expression</i>	参照ポイントとして使用する出力内の式です。

コマンドモード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、問題解決のためにテクニカル サポート担当者と直接作業している場合にだけ使用してください。このコマンドは、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。

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。



APPENDIX **D**

オープン ソース ソフトウェアについて

Cisco IOS ソフトウェアの pipe コマンドは、Henry Spencer の正規表現ライブラリ (regex) を使用しています。このライブラリの最新版は、ライブラリの旧バージョンとの互換性を保つために Catalyst オペレーティング システム ソフトウェアで若干修正されています。

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.



INDEX

A

aaa accounting dot1x コマンド [2-1](#)
aaa authentication dot1x コマンド [2-3](#)
aaa authorization network コマンド [2-5, 2-16, 2-21, 2-23, 2-25, 2-27, 2-112, 2-432, B-5, B-35](#)
AAA 方式 [2-3](#)
abort コマンド [2-772](#)
ACE [2-103, 2-367](#)
ACL
 deny [2-101](#)
 IP [2-172](#)
 許可 [2-365](#)
 非 IP プロトコル [2-269](#)
 表示 [2-415](#)
 レイヤ 2 インターフェイス [2-172](#)
apply コマンド [2-772](#)
archive download-sw コマンド [2-6](#)
archive tar コマンド [2-9](#)
archive upload-sw コマンド [2-12](#)
arp access-list コマンド [2-14](#)
authentication control-direction コマンド [2-16](#)
authentication event コマンド [2-18](#)
authentication failed VLAN
 「dot1x auth-fail vlan」を参照
authentication fallback コマンド [2-21](#)
authentication host-mode コマンド [2-23](#)
authentication open コマンド [2-25](#)
authentication order コマンド [2-27](#)
authentication periodic コマンド [2-29](#)
authentication port-control コマンド [2-31](#)
authentication priority コマンド [2-33](#)
authentication timer コマンド [2-35](#)

authentication violation コマンド [2-37](#)
auth-fail max-attempts
 「dot1x auth-fail max-attempts」を参照
auth-fail vlan
 「dot1x auth-fail vlan」を参照
auth open コマンド [2-25](#)
auth order コマンド [2-27](#)
auth timer コマンド [2-35](#)
auto qos voip コマンド [2-39](#)

B

BackboneFast、STP 用 [2-654](#)
boot config-file コマンド [2-44](#)
boot enable-break コマンド [2-45](#)
boot helper-config file コマンド [2-47](#)
boot helper コマンド [2-46](#)
boot manual コマンド [2-48](#)
boot private-config-file コマンド [2-49](#)
boot system コマンド [2-50](#)
boot (ブートローダ) コマンド [A-2](#)
BPDU [2-656](#)
BPDU ガード、スパニング ツリー用 [2-658, 2-692](#)
BPDU フィルタリング、スパニング ツリー用 [2-656, 2-692](#)

C

cat (ブートローダ) コマンド [A-4](#)
channel-group コマンド [2-51](#)
channel-protocol コマンド [2-55](#)
Cisco SoftPhone
 Auto-QoS の設定 [2-39](#)

- 送信されたパケットを信頼する **2-337**
- CISP
「Client Information Signalling Protocol」を参照
- cisp
debug platform cisp コマンド **B-35**
- cisp enable コマンド **2-56**
- class-map コマンド **2-59**
- Class of Service
「CoS」を参照
- class コマンド **2-57**
- clear dot1x コマンド **2-61**
- clear eap sessions コマンド **2-62**
- clear energywise neighbors コマンド **2-63**
- clear errdisable interface **2-64**
- clear ip arp inspection log コマンド **2-65**
- clear ip arp inspection statistics コマンド **2-66**
- clear ip dhcp snooping database コマンド **2-67**
- clear lacp コマンド **2-69**
- clear mac address-table コマンド **2-70, 2-72**
- clear nmsp statistics コマンド **2-73**
- clear pagp コマンド **2-74**
- clear port-security コマンド **2-75**
- clear spanning-tree counters コマンド **2-77**
- clear spanning-tree detected-protocols コマンド **2-78**
- clear vmpls statistics コマンド **2-80**
- clear vtp counters コマンド **2-81**
- Client Information Signalling Protocol **2-56, 2-112, 2-432, B-5, B-35**
- cluster commander-address コマンド **2-82**
- cluster discovery hop-count コマンド **2-84**
- cluster enable コマンド **2-85**
- cluster holdtime コマンド **2-86**
- cluster member コマンド **2-87**
- cluster outside-interface コマンド **2-89**
- cluster run コマンド **2-90**
- cluster standby-group コマンド **2-91**
- cluster timer コマンド **2-93**
- config-vlan モード
コマンド **2-759**
- サマリー **1-2**
- 説明 **1-4**
- 入力 **2-758**
- copy (ブートローダ) コマンド **A-5**
- CoS
着信値の上書き **2-307**
着信パケットへのデフォルト値の割り当て **2-307**
- CoS/DSCP マップ **2-311**
- CPU ASIC 統計、表示 **2-440**
- crashinfo ファイル **2-160**
-
- ## D
- debug auto qos コマンド **B-2**
- debug backup コマンド **B-4**
- debug cisp コマンド **B-5**
- debug cluster コマンド **B-6**
- debug dot1x コマンド **B-8**
- debug dtp コマンド **B-10**
- debug eap コマンド **B-11**
- debug etherchannel コマンド **B-12**
- debug ilpower コマンド **B-14**
- debug interface コマンド **B-15**
- debug ip dhcp snooping コマンド **B-17**
- debug ip igmp filter コマンド **B-18**
- debug ip igmp max-groups コマンド **B-19**
- debug ip igmp snooping コマンド **B-20**
- debug lacp コマンド **B-21**
- debug lldp packets コマンド **B-22**
- debug mac-notification コマンド **B-23**
- debug matm move update コマンド **B-25**
- debug matm コマンド **B-24**
- debug monitor コマンド **B-26**
- debug mvrdbg コマンド **B-28**
- debug nmsp コマンド **B-30**
- debug nvram コマンド **B-31**
- debug pagp コマンド **B-32**
- debug platform acl コマンド **B-33**
- debug platform backup interface コマンド **B-34**

- debug platform cisp コマンド [B-35](#)
- debug platform configuration コマンド [B-41](#)
- debug platform cpu-queues コマンド [B-36](#)
- debug platform dot1x コマンド [B-38](#)
- debug platform etherchannel コマンド [B-39](#)
- debug platform forw-tcam コマンド [B-40](#)
- debug platform ip arp inspection コマンド [B-43](#)
- debug platform ip dhcp コマンド [B-44](#)
- debug platform ip igmp snooping コマンド [B-45](#)
- debug platform ip source-guard コマンド [B-47](#)
- debug platform led コマンド [B-48](#)
- debug platform matm コマンド [B-49](#)
- debug platform messaging application コマンド [B-51](#)
- debug platform phy コマンド [B-52](#)
- debug platform pm コマンド [B-54](#)
- debug platform port-asic コマンド [B-56](#)
- debug platform port-security コマンド [B-57](#)
- debug platform qos-acl-tcam コマンド [B-58](#)
- debug platform resource-manager コマンド [B-59](#)
- debug platform snmp コマンド [B-60](#)
- debug platform span コマンド [B-61](#)
- debug platform supervisor-asic コマンド [B-62](#)
- debug platform sw-bridge コマンド [B-63](#)
- debug platform tcam コマンド [B-64](#)
- debug platform udld コマンド [B-66](#)
- debug platform vlan コマンド [B-67](#)
- debug pm コマンド [B-68](#)
- debug port-security コマンド [B-70](#)
- debug qos-manager コマンド [B-71](#)
- debug spanning-tree backbonefast コマンド [B-74](#)
- debug spanning-tree bpdu-opt コマンド [B-76](#)
- debug spanning-tree bpdu コマンド [B-75](#)
- debug spanning-tree mstp コマンド [B-77](#)
- debug spanning-tree switch コマンド [B-79](#)
- debug spanning-tree uplinkfast コマンド [B-81](#)
- debug spanning-tree コマンド [B-72](#)
- debug sw-vlan ifs コマンド [B-84](#)
- debug sw-vlan notification コマンド [B-86](#)
- debug sw-vlan vtp コマンド [B-87](#)
- debug sw-vlan コマンド [B-82](#)
- debug udld コマンド [B-89](#)
- debug vqpc コマンド [B-91](#)
- define interface-range コマンド [2-95](#)
- delete コマンド [2-97](#)
- delete (ブートローダ) コマンド [A-6](#)
- deny (ARP アクセス リスト コンフィギュレーション) コマンド [2-99](#)
- deny コマンド [2-101](#)
- DHCP スヌーピング
- イネーブル化
 - VLAN 上 [2-208](#)
 - インターフェイス上で信頼 [2-206](#)
 - オプション 82 [2-200, 2-202](#)
 - エッジ スイッチからの信頼できないパケットの受け入れ [2-202](#)
 - エラー回復タイマー [2-157](#)
 - レート制限 [2-204](#)
- DHCP スヌーピング バインディング データベース
- 更新 [2-395](#)
 - データベース エージェント、設定 [2-197](#)
 - データベース エージェントの統計情報のクリア [2-67](#)
 - バインディング
 - 削除 [2-195](#)
 - 追加 [2-195](#)
 - 表示 [2-500](#)
 - バインディング ファイル、設定 [2-197](#)
 - 表示
 - データベース エージェント ステータス [2-503, 2-505](#)
 - バインディング エントリ [2-500](#)
- dir (ブートローダ) コマンド [A-7](#)
- dot1x auth-fail max-attempts [2-106](#)
- dot1x auth-fail vlan [2-108](#)
- dot1x control-direction コマンド [2-110](#)
- dot1x credentials (グローバル コンフィギュレーション) コマンド [2-112](#)
- dot1x critical global configuration コマンド [2-113](#)
- dot1x critical interface configuration コマンド [2-115](#)

- dot1x default コマンド [2-117](#)
dot1x fallback コマンド [2-118](#)
dot1x guest-vlan コマンド [2-119](#)
dot1x host-mode コマンド [2-121](#)
dot1x initialize コマンド [2-123](#)
dot1x mac-auth-bypass コマンド [2-124](#)
dot1x max-reauth-req コマンド [2-126](#)
dot1x max-req コマンド [2-127](#)
dot1x pae コマンド [2-128](#)
dot1x port-control コマンド [2-129](#)
dot1x re-authenticate コマンド [2-131](#)
dot1x reauthentication コマンド [2-132](#)
dot1x test eapol-capable コマンド [2-133](#)
dot1x test timeout コマンド [2-134](#)
dot1x timeout コマンド [2-135](#)
dot1x violation-mode コマンド [2-138](#)
dot1x コマンド [2-104](#)
DSCP/CoS マップ [2-311](#)
DSCP/DSCP 変換マップ [2-311](#)
DTP [2-723](#)
DTP ネゴシエーション [2-725](#)
DTP フラップ
エラー回復タイマー [2-157](#)
エラー検出 [2-151](#)
duplex コマンド [2-139](#)
dynamic auto VLAN メンバシップ モード [2-722](#)
dynamic desirable VLAN メンバシップ モード [2-722](#)
Dynamic Host Configuration Protocol (DHCP)
「DHCP スヌーピング」を参照
Dynamic Trunking Protocol
「DTP」を参照
-
- ## E
- EAP-Request/Identity フレーム
再送信するまでの時間 [2-135](#)
送信する最高回数 [2-127](#)
energywise domain コマンド [2-145](#)
energywise query コマンド [2-147](#)
energywise (グローバル コンフィギュレーション) コマンド [2-141](#), [2-143](#)
errdisable detect cause small-frame コマンド [2-154](#)
errdisable detect cause コマンド [2-151](#)
errdisable recovery cause small-frame [2-156](#)
errdisable recovery コマンド [2-157](#)
errdisable インターフェイス、表示 [2-482](#)
errdisable 検出 [2-151](#)
EtherChannel
EtherChannel/PAgP のデバッグ、表示 [B-12](#)
LACP
システム プライオリティ [2-254](#)
チャンネル グループ情報のクリア [2-69](#)
デバッグ メッセージ、表示 [B-21](#)
表示 [2-532](#)
プロトコルの制限 [2-55](#)
ホットスタンバイ ポートのポート プライオリティ [2-252](#)
モード [2-51](#)
PAgP
エラー回復タイマー [2-157](#)
エラー検出 [2-151](#)
学習方式 [2-359](#)
集約ポート ラーナー [2-359](#)
送信トラフィックのインターフェイスのプライオリティ [2-361](#)
チャンネル グループ情報のクリア [2-74](#)
デバッグ メッセージ、表示 [B-32](#)
表示 [2-592](#)
物理ポート ラーナー [2-359](#)
モード [2-51](#)
イーサネット インターフェイスのチャンネル グループへの割り当て [2-51](#)
インターフェイス情報、表示 [2-482](#)
表示 [2-475](#)
負荷分散方式 [2-374](#)
プラットフォーム特定イベントのデバッグ、表示 [B-39](#)
ポート チャンネル論理インターフェイスの作成 [2-165](#)

exception crashinfo コマンド [2-160](#)

exit コマンド [2-772](#)

F

fallback profile コマンド [2-161](#)

flash_init (ブートローダ) コマンド [A-9](#)

Flex Link

設定 [2-716](#)

表示 [2-482](#)

優先 VLAN の設定 [2-719](#)

flowcontrol コマンド [2-163](#)

format (ブートローダ) コマンド [A-10](#)

fsck (ブートローダ) コマンド [A-11](#)

H

help (ブートローダ) コマンド [A-12](#)

Hot Standby Router Protocol

「HSRP」を参照

HSRP

HSRP グループのクラスタへのバインド [2-91](#)

スタンバイ グループ [2-91](#)

I

IEEE 802.1x

「ポートベース認証」も参照

違反エラーの回復 [2-157](#)

スイッチポート モード [2-723](#)

IEEE 802.1x 対応ポートの再認証 [2-131](#)

IEEE 802.1x ポートベース認証

ゲスト VLAN サプリカントのイネーブル化 [2-107,](#)
[2-118, 2-162](#)

IGMP グループ、最大数の設定 [2-211](#)

IGMP 最大グループ、デバッグ [B-19](#)

IGMP スヌーピング

イネーブル化 [2-215](#)

インターフェイスのトポロジ変更通知動作 [2-225](#)

クエリア [2-219](#)

クエリー要求 [2-223](#)

グループのスタティック メンバーとしてのポートを
追加 [2-230](#)

スイッチのトポロジ変更通知動作 [2-223](#)

設定可能な Leave タイマーのイネーブル化 [2-217](#)

即時脱退機能のイネーブル化 [2-226](#)

表示 [2-509, 2-514, 2-516](#)

フラッドイング クエリー カウント [2-223](#)

マルチキャスト テーブル [2-512](#)

レポート抑制 [2-221](#)

IGMP フィルタ

適用 [2-209](#)

デバッグ メッセージ、表示 [B-18](#)

IGMP プロファイル

作成 [2-213](#)

表示 [2-508](#)

interface port-channel コマンド [2-165](#)

interface range コマンド [2-167](#)

interface vlan コマンド [2-170](#)

ip access-group コマンド [2-172](#)

ip address コマンド [2-174](#)

ip admission name proxy http コマンド [2-178](#)

ip admission コマンド [2-176](#)

ip arp inspection filter vlan コマンド [2-180](#)

ip arp inspection limit コマンド [2-182](#)

ip arp inspection log-buffer コマンド [2-184](#)

ip arp inspection trust コマンド [2-186](#)

ip arp inspection validate コマンド [2-188](#)

ip arp inspection vlan logging コマンド [2-191](#)

ip arp inspection vlan コマンド [2-190](#)

ip dhcp snooping binding コマンド [2-195](#)

ip dhcp snooping database コマンド [2-197](#)

ip dhcp snooping information option allow-untrusted コマ
ンド [2-202](#)

ip dhcp snooping information option コマンド [2-200](#)

ip dhcp snooping limit rate コマンド [2-204](#)

ip dhcp snooping trust コマンド [2-206](#)

ip dhcp snooping verify コマンド [2-207](#)

ip dhcp snooping vlan コマンド [2-208](#)
 ip dhcp snooping コマンド [2-194](#)
 IP DHCP スヌーピング
 「DHCP スヌーピング」を参照
 ip igmp filter コマンド [2-209](#)
 ip igmp max-groups コマンド [2-211](#)
 ip igmp profile コマンド [2-213](#)
 ip igmp snooping last-member-query-interval コマ
 ンド [2-217](#)
 ip igmp snooping querier コマンド [2-219](#)
 ip igmp snooping report-suppression コマンド [2-221](#)
 ip igmp snooping tcn flood コマンド [2-225](#)
 ip igmp snooping tcn コマンド [2-223](#)
 ip igmp snooping vlan immediate-leave コマンド [2-226](#)
 ip igmp snooping vlan mrouter コマンド [2-228](#)
 ip igmp snooping vlan static コマンド [2-230](#)
 ip igmp snooping コマンド [2-215](#)
 IP Phone
 Auto-QoS の設定 [2-39](#)
 送信されたパケットを信頼する [2-337](#)
 IP Precedence/DSCP マップ [2-311](#)
 ip source binding コマンド [2-232](#)
 ip ssh コマンド [2-234](#)
 ipv6 mld snooping last-listener-query count コマン
 ンド [2-240](#)
 ipv6 mld snooping last-listener-query-interval コマン
 ンド [2-242](#)
 ipv6 mld snooping listener-message-suppression コマン
 ンド [2-244](#)
 ipv6 mld snooping robustness-variable コマンド [2-246](#)
 ipv6 mld snooping tcn コマンド [2-248](#)
 ipv6 mld snooping vlan コマンド [2-250](#)
 ipv6 mld snooping コマンド [2-238](#)
 IPv6 SDM テンプレート [2-400](#)
 ip verify source コマンド [2-236](#)
 IP アドレス、設定 [2-174](#)
 IP ソース ガード
 イネーブル化 [2-236](#)
 スタティック IP ソース バインディング [2-232](#)
 ディセーブル化 [2-236](#)

表示

設定 [2-520](#)ダイナミック バインディング エントリの
み [2-500](#)バインディング エントリ [2-518](#)IP マルチキャスト アドレス [2-344](#)

L

LACP

「EtherChannel」を参照

lacp port-priority コマンド [2-252](#)lacp system-priority コマンド [2-254](#)

Link Aggregation Control Protocol

「EtherChannel」を参照

link state group コマンド [2-260](#)link state track コマンド [2-262](#)location (インターフェイス コンフィギュレーション) コ
マンド [2-258](#)location (グローバル コンフィギュレーション) コマン
ド [2-256](#)logging event power-inline-status コマンド [2-264](#)logging event コマンド [2-263](#)logging file コマンド [2-265](#)

M
mac access-group コマンド [2-267](#)mac access-list extended コマンド [2-269](#)mac address-table aging-time [2-267](#)mac address-table aging-time コマンド [2-271](#)mac address-table learning コマンド [2-272](#)mac address-table move update コマンド [2-274](#)mac address-table notification コマンド [2-276](#)mac address-table static drop コマンド [2-279](#)mac address-table static コマンド [2-278](#)macro apply コマンド [2-281](#)macro auto execute コマンド [2-284](#)macro auto global processing コマンド [2-289](#)

- macro description コマンド [2-291](#)
- macro global description コマンド [2-295](#)
- macro global コマンド [2-292](#)
- macro name コマンド [2-296](#)
- MAC アクセス グループ、表示 [2-541](#)
- MAC アクセス リスト [2-101](#)
- MAC アクセス リスト コンフィギュレーション モード [2-269](#)
- MAC アドレス
 - MAC アドレス通知のイネーブル化 [2-276](#)
 - MAC アドレス テーブル移行更新のイネーブル化 [2-274](#)
 - VLAN ごとの MAC アドレス学習のディセーブル化 [2-272](#)
 - スタティック
 - インターフェイス上でドロップ [2-279](#)
 - 追加および削除 [2-278](#)
 - 表示 [2-560](#)
 - ダイナミック
 - エージング タイム [2-271](#)
 - 削除 [2-70](#)
 - 表示 [2-551](#)
 - テーブル [2-545](#)
 - 表示
 - MAC アドレス テーブル移行更新 [2-556](#)
 - VLAN ごと [2-562](#)
 - VLAN のアドレス数 [2-549](#)
 - インターフェイス単位 [2-553](#)
 - エージング タイム [2-547](#)
 - スタティック [2-560](#)
 - スタティック エントリおよびダイナミック エントリ [2-543](#)
 - すべて [2-545](#)
 - ダイナミック [2-551](#)
 - 通知設定 [2-555, 2-558](#)
- MAC アドレス通知、デバッグ [B-23](#)
- match (クラスマップ コンフィギュレーション) コマンド [2-298](#)
- Maximum Transmission Unit
 - 「MTU」を参照
- mdix auto コマンド [2-300](#)
- media-type コマンド [2-301](#)
- memory (ブートローダ) コマンド [A-13](#)
- mkdir (ブートローダ) コマンド [A-14](#)
- MLD スヌーピング
 - イネーブル化 [2-238](#)
 - クエリーの設定 [2-240, 2-242](#)
 - 設定 [2-244, 2-246](#)
 - トポロジ変更通知の設定 [2-248](#)
 - 表示 [2-522, 2-524, 2-526, 2-528](#)
- mls qos aggregate-policer コマンド [2-305](#)
- mls qos cos コマンド [2-307](#)
- mls qos dscp-mutation コマンド [2-309](#)
- mls qos map コマンド [2-311](#)
- mls qos queue-set output buffers コマンド [2-315](#)
- mls qos queue-set output threshold コマンド [2-317](#)
- mls qos rewrite ip dscp コマンド [2-319](#)
- mls qos srr-queue input bandwidth コマンド [2-321](#)
- mls qos srr-queue input buffers コマンド [2-323](#)
- mls qos srr-queue input cos-map コマンド [2-325](#)
- mls qos srr-queue input dscp-map コマンド [2-327](#)
- mls qos srr-queue input priority-queue コマンド [2-329](#)
- mls qos srr-queue input threshold コマンド [2-331](#)
- mls qos srr-queue output cos-map コマンド [2-333](#)
- mls qos srr-queue output dscp-map コマンド [2-335](#)
- mls qos trust コマンド [2-337](#)
- mls qos コマンド [2-303](#)
- Mode ボタン、パスワード回復 [2-402](#)
- monitor session コマンド [2-339](#)
- more (ブートローダ) コマンド [A-15](#)
- MSTP
 - MST リージョン
 - MST コンフィギュレーション モード [2-674](#)
 - VLAN とインスタンス間のマッピング [2-674](#)
 - 現在または保留中の設定の表示 [2-674](#)
 - コンフィギュレーション リビジョン番号 [2-674](#)
 - 設定名 [2-674](#)
 - 表示 [2-613](#)

変更の中止 [2-674](#)
 変更の適用 [2-674](#)
 ステート情報の表示 [2-612](#)
 ステート変更
 BPDU ガードのイネーブル化 [2-658, 2-692](#)
 BPDU フィルタリングのイネーブル化 [2-656, 2-692](#)
 PortFast 対応ポートのシャットダウン [2-692](#)
 PortFast のイネーブル化 [2-692, 2-695](#)
 転送遅延時間 [2-678](#)
 フォワーディング ステートへの高速移行 [2-668](#)
 ブロッキング ステートからフォワーディング ステートへ [2-695](#)
 リスニングおよびラーニング ステートの期間 [2-678](#)
 相互運用 [2-78](#)
 パス コスト [2-676](#)
 表示 [2-613](#)
 プロトコル移行プロセスの再開 [2-78](#)
 プロトコル モード [2-672](#)
 リンク タイプ [2-668](#)
 ルート スイッチ
 BPDU ドロップまでの最大ホップ数 [2-682](#)
 BPDU メッセージの間隔 [2-680](#)
 hello BPDU メッセージの間隔 [2-679, 2-688](#)
 hello タイム [2-679, 2-688](#)
 拡張システム ID の影響 [2-664](#)
 スイッチ プライオリティ [2-687](#)
 選択に関するポート プライオリティ [2-684](#)
 プライマリまたはセカンダリ [2-688](#)
 有効期限 [2-680](#)
 ルート ポート
 指定ポートの制限 [2-666](#)
 ルート ガード [2-666](#)
 ルートとなるポートの制限 [2-666](#)
 ループ ガード [2-666](#)
 MTU
 グローバル設定の表示 [2-621](#)
 サイズの設定 [2-743](#)

Multicast Listener Discovery

「MLD」を参照

Multicast VLAN Registration

「MVR」を参照

Multiple Spanning Tree Protocol

「MSTP」を参照

MVR

アドレスのエイリアス [2-345](#)

インターフェイス情報の表示 [2-583](#)

インターフェイスの設定 [2-347](#)

設定 [2-344](#)

デバッグ メッセージ、表示 [B-28](#)

表示 [2-581](#)

メンバー、表示 [2-585](#)

mvr vlan group コマンド [2-348](#)

mvr (インターフェイス コンフィギュレーション) コマンド [2-347](#)

mvr (グローバル コンフィギュレーション) コマンド [2-344](#)

N

『Network Admission Control Software Configuration Guide』 [2-177, 2-179](#)

network-policy profile (ネットワーク ポリシー コンフィギュレーション) コマンド [2-354](#)

network-policy (グローバル コンフィギュレーション) コマンド [2-352](#)

network-policy コマンド [2-350](#)

nmosp attachment suppress コマンド [2-358](#)

nmosp コマンド [2-356](#)

nonegotiate、速度 [2-703](#)

no vlan コマンド [2-758, 2-769](#)

P

PAGP

「EtherChannel」を参照

pagp learn-method コマンド [2-359](#)

pagp port-priority コマンド [2-361](#)

- permit (ARP アクセス リスト コンフィギュレーション)
 コマンド [2-363](#)
- permit (MAC アクセス リスト コンフィギュレーション)
 コマンド [2-365](#)
- Per-VLAN Spanning-Tree Plus
 「STP」を参照
- PID、表示 [2-494](#)
- PIM-DVMRP、マルチキャスト ルータ 学習方式 [2-228](#)
- PoE
 コントローラ レジスタ値の表示 [2-449](#)
 状態のロギング [2-264](#)
 電力管理情報の表示 [2-602](#)
 電力管理モードの設定 [2-376](#)
 電力消費のポリシング [2-381](#)
 電力のモニタリング [2-381](#)
 パワー バジレットの設定 [2-379](#)
- police aggregate コマンド [2-370](#)
- police コマンド [2-368](#)
- policy-map コマンド [2-372](#)
- port-channel load-balance コマンド [2-374](#)
- PortFast、スパニング ツリー用 [2-695](#)
- power inline consumption コマンド [2-379](#)
- power inline police コマンド [2-381](#)
- power inline コマンド [2-376](#)
- Power over Ethernet
 「PoE」を参照
- priority-queue コマンド [2-384](#)
- PVST+
 「STP」を参照
-
- Q**
- QoS
 auto-QoS
 設定 [2-39](#)
 デバッグ メッセージ、表示 [B-2](#)
 表示 [2-424](#)
- DSCP 透過性 [2-319](#)
- DSCP の信頼できるポート
 DSCP/DSCP 変換マップの定義 [2-311](#)
 DSCP/DSCP 変換マップの適用 [2-309](#)
- IP Phone の信頼される境界 [2-337](#)
- イネーブル化 [2-303](#)
- キュー、緊急キューのイネーブル化 [2-384](#)
- クラス マップ
 一致基準の定義 [2-298](#)
 作成 [2-59](#)
 表示 [2-433](#)
- 出力キュー
 CoS 出力キューのしきい値マップの定義 [2-333](#)
 CoS 出力キューのしきい値マップの表示 [2-572](#)
 CoS 値のキューおよびしきい値のマッピング [2-333](#)
 DSCP 出力キューしきい値マップの定義 [2-335](#)
 DSCP 出力キューしきい値マップの表示 [2-572](#)
 DSCP 値のキューおよびしきい値へのマッピング [2-335](#)
 WTD しきい値の設定 [2-317](#)
 キューイングの指針の表示 [2-568](#)
 キューセット設定の表示 [2-575](#)
 最大および予約済みメモリ割り当ての設定 [2-317](#)
 帯域幅共有とスケジューリングのイネーブル化 [2-709](#)
 帯域幅シェーピングとスケジューリングのイネーブル化 [2-707](#)
 バッファの割り当て [2-315](#)
 バッファ割り当ての表示 [2-568](#)
 ポートでの最大出力の制限 [2-705](#)
 ポートのキューセットへのマッピング [2-386](#)
- 設定情報の表示 [2-424, 2-564](#)
- 着信パケットの CoS 値の定義 [2-307](#)
- 統計
 キューに入れられた、または削除されたパケット [2-568](#)
 送受信された CoS 値 [2-568](#)
 送受信された DSCP 値 [2-568](#)

- プロファイル内とプロファイル外のパケット
ト **2-568**
- 入力キュー
- CoS 値のキューおよびしきい値のマッピング
グ **2-325**
 - CoS 入力キューのしきい値マップの定義
義 **2-325**
 - CoS 入力キューのしきい値マップの表示
示 **2-572**
 - DSCP 値のキューおよびしきい値へのマッピング
グ **2-327**
 - DSCP 入力キューしきい値マップの定義 **2-327**
 - DSCP 入力キューしきい値マップの表示 **2-572**
 - SRR スケジューリングの重みの割り当て
て **2-321**
 - WTD しきい値の設定 **2-331**
 - キューイングの指針の表示 **2-568**
 - 設定の表示 **2-566**
 - バッファの割り当て **2-323**
 - バッファ割り当ての表示 **2-568**
 - プライオリティ キューのイネーブル化 **2-329**
- ポートの信頼状態 **2-337**
- ポリシー マップ
- DSCP 値または IP precedence 値の設定 **2-406**
 - インターフェイスへの適用 **2-404, 2-408**
 - 階層 **2-373**
 - 作成 **2-372**
 - 集約ポリサーの適用 **2-370**
 - 信頼状態 **2-751**
 - トラフィックの分類 **2-57**
 - ポリサーの定義 **2-305, 2-368**
 - ポリサーの表示 **2-565**
 - ポリシー マップの表示 **2-597**
 - ポリシング設定 DSCP マップ **2-311**
- マップ
- 定義 **2-311, 2-325, 2-327, 2-333, 2-335**
 - 表示 **2-572**
- QoS の信頼される境界 **2-337**
- QoS のポートの信頼状態 **2-337**
- Quality of Service
- 「QoS」を参照
- queue-set コマンド **2-386**
-
- ## R
- radius-server dead-criteria コマンド **2-387**
 - radius-server host コマンド **2-389**
 - Rapid Per-VLAN Spanning-Tree Plus
「STP」を参照
 - Rapid PVST+
「STP」を参照
 - rcommand コマンド **2-391**
 - remote-span コマンド **2-393**
 - rename (ブートローダ) コマンド **A-16**
 - renew ip dhcp snooping database コマンド **2-395**
 - reset コマンド **2-772**
 - reset (ブートローダ) コマンド **A-17**
 - rmdir (ブートローダ) コマンド **A-18**
 - rmon collection stats コマンド **2-399**
 - RSPAN
 - remote-span コマンド **2-393**
 - RSPAN トラフィックのフィルタリング
セッション
表示 **2-578**
 - 設定 **2-339**
 - 表示 **2-578**
-
- ## S
- sdm prefer コマンド **2-400**
 - SDM テンプレート
 - デュアル IPv4/IPv6 **2-400**
 - 表示 **2-606**
 - service password-recovery コマンド **2-402**
 - service-policy コマンド **2-404**
 - setup express コマンド **2-411**
 - setup コマンド **2-408**
 - set コマンド **2-406**
 - set (ブートローダ) コマンド **A-19**
 - shell trigger コマンド **2-413**

- show access-lists コマンド [2-415](#)
- show archive status コマンド [2-418](#)
- show arp access-list コマンド [2-419](#)
- show authentication コマンド [2-420](#)
- show auto qos コマンド [2-424](#)
- show boot コマンド [2-428](#)
- show cable-diagnostics tdr コマンド [2-430](#)
- show changes コマンド [2-772](#)
- show cisp コマンド [2-432](#)
- show class-map コマンド [2-433](#)
- show cluster candidates コマンド [2-436](#)
- show cluster members コマンド [2-438](#)
- show cluster コマンド [2-434](#)
- show controllers cpu-interface コマンド [2-440](#)
- show controllers ethernet-controller コマンド [2-442](#)
- show controllers power inline コマンド [2-449](#)
- show controllers team コマンド [2-451](#)
- show controller utilization コマンド [2-453](#)
- show current コマンド [2-772](#)
- show dot1x コマンド [2-455](#)
- show dtp [2-459](#)
- show eap コマンド [2-461](#)
- show energywise コマンド [2-464](#)
- show env コマンド [2-468](#)
- show errdisable detect コマンド [2-469](#)
- show errdisable flap-values コマンド [2-471](#)
- show errdisable recovery コマンド [2-473](#)
- show etherchannel コマンド [2-475](#)
- show fallback profile コマンド [2-478](#)
- show flowcontrol コマンド [2-480](#)
- show interfaces counters コマンド [2-491](#)
- show interfaces コマンド [2-482](#)
- show inventory コマンド [2-494](#)
- show ip arp inspection コマンド [2-495](#)
- show ip dhcp snooping binding コマンド [2-500](#)
- show ip dhcp snooping database コマンド [2-503, 2-505](#)
- show ip dhcp snooping コマンド [2-499](#)
- show ip igmp profile コマンド [2-508](#)
- show ip igmp snooping address コマンド [2-524](#)
- show ip igmp snooping groups コマンド [2-512](#)
- show ip igmp snooping mrouter コマンド [2-514, 2-526](#)
- show ip igmp snooping querier コマンド [2-516, 2-528](#)
- show ip igmp snooping コマンド [2-509, 2-522](#)
- show ip source binding コマンド [2-518](#)
- show ipv6 route updated [2-530](#)
- show ip verify source コマンド [2-520](#)
- show lacp コマンド [2-532](#)
- show link state group コマンド [2-539](#)
- show location [2-536](#)
- show mac access-group コマンド [2-541](#)
- show mac address-table address コマンド [2-545](#)
- show mac address-table aging time コマンド [2-547](#)
- show mac address-table count コマンド [2-549](#)
- show mac address-table dynamic コマンド [2-551](#)
- show mac address-table interface コマンド [2-553](#)
- show mac address-table learning コマンド [2-555](#)
- show mac address-table move update コマンド [2-556](#)
- show mac address-table notification コマンド [2-72, 2-558, B-25](#)
- show mac address-table static コマンド [2-560](#)
- show mac address-table vlan コマンド [2-562](#)
- show mac address-table コマンド [2-543](#)
- show mls qos aggregate-policer コマンド [2-565](#)
- show mls qos input-queue コマンド [2-566](#)
- show mls qos interface コマンド [2-568](#)
- show mls qos maps コマンド [2-572](#)
- show mls qos queue-set コマンド [2-575](#)
- show mls qos vlan コマンド [2-577](#)
- show mls qos コマンド [2-564](#)
- show monitor コマンド [2-578](#)
- show mvr interface コマンド [2-583](#)
- show mvr members コマンド [2-585](#)
- show mvr コマンド [2-581](#)
- show network-policy profile コマンド [2-587](#)
- show nmsp コマンド [2-589](#)
- show pagp コマンド [2-592](#)
- show parser macro コマンド [2-594](#)
- show platform acl コマンド [C-2](#)

- show platform backup interface コマンド **C-3**
- show platform etherchannel コマンド **C-4**
- show platform forward コマンド **C-5**
- show platform igmp snooping コマンド **C-7**
- show platform layer4op コマンド **C-9**
- show platform mac-address-table コマンド **C-10**
- show platform messaging コマンド **C-11**
- show platform monitor コマンド **C-12**
- show platform mvr table コマンド **C-13**
- show platform pm コマンド **C-14**
- show platform port-asic コマンド **C-16**
- show platform port-security コマンド **C-20**
- show platform qos コマンド **C-21**
- show platform resource-manager コマンド **C-22**
- show platform snmp counters コマンド **C-24**
- show platform spanning-tree コマンド **C-25**
- show platform stack manager コマンド **C-27**
- show platform stp-instance コマンド **C-26**
- show platform team コマンド **C-28**
- show platform vlan コマンド **C-30**
- show policy-map コマンド **2-597**
- show port security コマンド **2-599**
- show power inline コマンド **2-602**
- show proposed コマンド **2-772**
- show sdm prefer コマンド **2-606**
- show setup express コマンド **2-608**
- show shell コマンド **2-609**
- show spanning-tree コマンド **2-612**
- show storm-control コマンド **2-618**
- show system mtu コマンド **2-621**
- show trust コマンド **2-751**
- show uddl コマンド **2-623**
- show version コマンド **2-626**
- show vlan コマンド **2-628**
- show vlan コマンド、フィールド **2-629**
- show vmps コマンド **2-631**
- show vtp コマンド **2-634**
- shutdown vlan コマンド **2-640**
- shutdown コマンド **2-639**
- small violation-rate コマンド **2-641**
- Smartports マクロ
「マクロ」を参照
- snmp-server enable traps コマンド **2-643**
- snmp-server host コマンド **2-647**
- snmp trap mac-notification コマンド **2-652**
- SNMP 通知、送信のイネーブル化 **2-643**
- SNMP トラップ
MAC アドレス通知機能のイネーブル化 **2-276**
MAC アドレス通知トラップのイネーブル化 **2-652**
送信のイネーブル化 **2-643**
- SNMP ホスト、指定 **2-647**
- SoftPhone
「Cisco SoftPhone」を参照
- SPAN
SPAN トラフィックのフィルタリング **2-339**
セッション
インターフェイスの追加 **2-339**
新規開始 **2-339**
表示 **2-578**
設定 **2-339**
デバッグ メッセージ、表示 **B-26**
表示 **2-578**
- spanning-tree backbonefast コマンド **2-654**
- spanning-tree bpdupfilter コマンド **2-656**
- spanning-tree bpduguard コマンド **2-658**
- spanning-tree cost コマンド **2-660**
- spanning-tree etherchannel コマンド **2-662**
- spanning-tree extend system-id コマンド **2-664**
- spanning-tree guard コマンド **2-666**
- spanning-tree link-type コマンド **2-668**
- spanning-tree loopguard default コマンド **2-670**
- spanning-tree mode コマンド **2-672**
- spanning-tree mst configuration コマンド **2-674**
- spanning-tree mst cost コマンド **2-676**
- spanning-tree mst forward-time コマンド **2-678**
- spanning-tree mst hello-time コマンド **2-679**
- spanning-tree mst max-age コマンド **2-680**
- spanning-tree mst max-hops コマンド **2-682**

- spanning-tree mst port-priority コマンド [2-684](#)
- spanning-tree mst pre-standard コマンド [2-686](#)
- spanning-tree mst priority コマンド [2-687](#)
- spanning-tree mst root コマンド [2-688](#)
- spanning-tree portfast (インターフェイス コンフィギュレーション) コマンド [2-695](#)
- spanning-tree portfast (グローバル コンフィギュレーション) コマンド [2-692](#)
- spanning-tree port-priority コマンド [2-690](#)
- spanning-tree transmit hold-count コマンド [2-697](#)
- spanning-tree uplinkfast コマンド [2-698](#)
- spanning-tree vlan コマンド [2-700](#)
- speed コマンド [2-703](#)
- srr-queue bandwidth limit コマンド [2-705](#)
- srr-queue bandwidth share コマンド [2-709](#)
- SSH、バージョンの設定 [2-234](#)
- storm-control コマンド [2-711](#)
- STP
 - BackboneFast [2-654](#)
 - EtherChannel の設定ミス [2-662](#)
 - VLAN オプション [2-687, 2-700](#)
 - カウンタ、クリア [2-77](#)
 - 拡張システム ID [2-664](#)
 - 間接リンク障害の検出 [2-654](#)
 - ステート情報の表示 [2-612](#)
 - ステート変更
 - BPDU ガードのイネーブル化 [2-658, 2-692](#)
 - BPDU フィルタリングのイネーブル化 [2-656, 2-692](#)
 - PortFast 対応ポートのシャットダウン [2-692](#)
 - PortFast のイネーブル化 [2-692, 2-695](#)
 - エラー ステートから回復するタイマーのイネーブル化 [2-157](#)
 - 転送遅延時間 [2-700](#)
 - ブロッキング ステートからフォワーディング ステートへ [2-695](#)
 - リスニングおよびラーニング ステートの期間 [2-700](#)
 - デバッグ メッセージ、表示
 - BackboneFast イベント [B-74](#)
- MSTP [B-77](#)
- UplinkFast [B-81](#)
- 最適化された BPDU 処理 [B-76](#)
- スイッチ シム [B-79](#)
- スパニングツリー アクティビティ [B-72](#)
- 送受信された BPDU [B-75](#)
- パス コスト [2-660](#)
- プロトコル モード [2-672](#)
- ルート スイッチ
 - BPDU メッセージの間隔 [2-700](#)
 - hello BPDU メッセージの間隔 [2-700](#)
 - hello タイム [2-700](#)
 - 拡張システム ID の影響 [2-664, 2-701](#)
 - スイッチ プライオリティ [2-700](#)
 - 選択に関するポート プライオリティ [2-690](#)
 - プライマリまたはセカンダリ [2-700](#)
 - 有効期限 [2-700](#)
- ルート ポート
 - UplinkFast [2-698](#)
 - 新しいルート ポートの選択の高速化 [2-698](#)
 - 指定ポートの制限 [2-666](#)
 - ルート ガード [2-666](#)
 - ルートとなるポートの制限 [2-666](#)
 - ループ ガード [2-666](#)
- STP の拡張システム ID [2-664](#)
- switchport access コマンド [2-714](#)
- switchport backup interface コマンド [2-716](#)
- switchport block コマンド [2-720](#)
- switchport host コマンド [2-721](#)
- switchport mode コマンド [2-722](#)
- switchport nonegotiate コマンド [2-725](#)
- switchport port-security aging コマンド [2-732](#)
- switchport port-security コマンド [2-727](#)
- switchport priority extend コマンド [2-734](#)
- switchport protected コマンド [2-736](#)
- switchport trunk コマンド [2-738](#)
- switchport voice vlan コマンド [2-741](#)
- system mtu コマンド [2-743](#)

T

tar ファイル、作成、一覧表示、および抽出 **2-9**
 TDR、実行 **2-745**
 Telnet、クラスタ スイッチへの通信に使用 **2-391**
 test cable-diagnostics tdr コマンド **2-745**
 test relay **2-746**
 traceroute mac ip コマンド **2-749**
 traceroute mac コマンド **2-746**
 type (ブートローダ) コマンド **A-22**

U

UDLD

アグレッシブ モード **2-753, 2-755**
 インターフェイスごとのイネーブル化 **2-755**
 エラー回復タイマー **2-157**
 グローバルにイネーブ化 **2-753**
 シャットダウン インターフェイスのリセット **2-757**
 ステータス **2-623**
 デバッグ メッセージ、表示 **B-89**
 ノーマル モード **2-753, 2-755**
 メッセージ タイマー **2-753**
 udld port コマンド **2-755**
 udld reset コマンド **2-757**
 udld コマンド **2-753**
 unset (ブートローダ) コマンド **A-23**
 UplinkFast、STP 用 **2-698**

V

version (ブートローダ) コマンド **A-25**

VLAN

MAC アドレス

数 **2-549**

表示 **2-562**

VTP の SNMP トラップ **2-645, 2-649**

拡張範囲 **2-758**

ゲスト VLAN サプリカントのイネーブル化 **2-107, 2-118, 2-162**

コンフィギュレーションの保存 **2-758**

再起動 **2-640**

シャットダウン **2-640**

設定 **2-758, 2-764**

設定の表示 **2-628**

中断 **2-640**

追加 **2-758**

デバッグ メッセージ、表示

ISL **B-86**

VLAN IOS File System エラー テスト **B-84**

VLAN マネージャのアクティビティ **B-82**

VTP **B-87**

標準範囲 **2-758, 2-764**

変数 **2-764**

メディア タイプ **2-761, 2-766**

vlan database コマンド **2-771**

VLAN ID 範囲 **2-758, 2-764**

VLAN Query Protocol

「VQP」を参照

VLAN Trunking Protocol

「VTP」を参照

vlan (VLAN コンフィギュレーション) コマンド **2-764**

vlan (グローバル コンフィギュレーション) コマンド **2-758**

VLAN コンフィギュレーション

規則 **2-762, 2-767**

保存 **2-758, 2-768**

VLAN コンフィギュレーション モード

コマンド

VLAN **2-764**

VTP **2-783**

サマリー **1-2**

説明 **1-5**

入力 **2-771**

VLAN での MLD スヌーピング、イネーブル化 **2-250**

VLAN トランキング プロトコル

「VTP」を参照

VMPS

- エラー回復タイマー [2-158](#)
- サーバの設定 [2-777](#)
- ダイナミック VLAN 割り当ての再確認 [2-774](#)
- 表示 [2-631](#)
- vmmps reconfirm (グローバル コンフィギュレーション) コマンド [2-775](#)
- vmmps reconfirm (特権 EXEC) コマンド [2-774](#)
- vmmps retry コマンド [2-776](#)
- vmmps server コマンド [2-777](#)

VQP

- クライアント統計情報のクリア [2-80](#)
- サーバごとの再試行回数 [2-776](#)
- 再確認間隔 [2-775](#)
- 情報の表示 [2-631](#)
- ダイナミック VLAN 割り当ての再確認 [2-774](#)
- ダイナミック アクセス ポート [2-715](#)

VTP

- イネーブル化
 - バージョン 2 [2-779, 2-783](#)
 - プルーニング [2-779, 2-783](#)
- カウンタ表示フィールド [2-635](#)
- コンフィギュレーションの保存 [2-758, 2-768](#)
- 情報の表示 [2-634](#)
- ステータス [2-634](#)
- ステータス表示フィールド [2-637](#)
- 設定
 - ドメイン名 [2-779, 2-783](#)
 - パスワード [2-779, 2-783](#)
 - ファイル名 [2-779](#)
 - モード [2-779, 2-783](#)
- 統計 [2-634](#)
- 特性の変更 [2-779](#)
- プルーニング [2-779, 2-783](#)
- プルーニング カウンタのクリア [2-81](#)
- モード [2-779, 2-783](#)
- vtp (VLAN コンフィギュレーション) コマンド [2-783](#)
- vtp (グローバル コンフィギュレーション) コマンド [2-779](#)

あ

- アクセス グループ
 - IP [2-172](#)
 - MAC、表示 [2-541](#)
- アクセス コントロール エントリ
 - 「ACE」を参照
- アクセス コントロール リスト
 - 「ACL」を参照
- アクセス ポート [2-722](#)
- アクセス モード [2-722](#)
- アップグレード
 - ソフトウェア イメージ
 - ステータスのモニタリング [2-418](#)
 - ダウンロード [2-6](#)
- アドレスのエイリアス [2-345](#)

い

- イーサネット コントローラ、内部レジスタの表示 [2-442](#)
- イーサネット統計、収集 [2-399](#)
- イメージ
 - 「ソフトウェア イメージ」を参照
- インターネット グループ管理プロトコル
 - 「IGMP」を参照
- インターフェイス
 - MAC アドレス テーブルの表示 [2-553](#)
 - イーサネット インターフェイスのチャンネル グループへの割り当て [2-51](#)
 - 再起動 [2-639](#)
 - 作成、ポート チャンネル論理 [2-165](#)
 - 設定 [2-139](#)
 - 設定、複数 [2-167](#)
 - ディセーブル化 [2-639](#)
 - デバッグ メッセージ、表示 [B-15](#)
- インターフェイス コンフィギュレーションモード [1-2, 1-4](#)
- インターフェイスの速度、設定 [2-703](#)
- インターフェイス範囲マクロ [2-95](#)

え

エラー条件、表示 [2-471](#)

お

音声 VLAN

設定 [2-741](#)

ポート プライオリティの設定 [2-734](#)

温度情報、表示 [2-468](#)

オンライン診断

グローバル コンフィギュレーション モード

ヘルス モニタリング診断テストのスケジュールの
クリア [2-65](#)

ヘルス モニタリング診断テストのスケジュールの
設定 [2-65](#)

ヘルス モニタリング診断テストの設定 [2-65](#)

か

階層ポリシーマップ [2-373](#)

回復メカニズム

原因 [2-157](#)

タイマー間隔 [2-158](#)

表示 [2-64, 2-430, 2-469, 2-473](#)

拡張範囲 VLAN

許可 VLAN リスト [2-738](#)

設定 [2-758](#)

プルーニング適格リスト [2-738](#)

環境変数、表示 [2-428](#)

き

起動

Cisco IOS イメージ [2-50](#)

環境変数の表示 [2-428](#)

手動 [2-48](#)

中断 [2-45](#)

許可 VLAN リスト [2-738](#)

く

クエリー時間、MVR [2-344](#)

クラスタ

HSRP グループへのバインド [2-91](#)

HSRP スタンバイ グループ [2-91](#)

SNMP トラップ [2-643](#)

拡張検出用にホップカウント制限 [2-84](#)

候補の追加 [2-87](#)

冗長 [2-91](#)

通信

Telnet を使用したメンバー [2-391](#)

クラスタ外部のデバイス [2-89](#)

デバッグ メッセージ、表示 [B-6](#)

入力して設定 [2-87](#)

表示

候補スイッチ [2-436](#)

ステータス [2-434](#)

デバッグ メッセージ [B-6](#)

メンバー スイッチ [2-438](#)

クラスタ スイッチの冗長 [2-91](#)

クラスタのホップ カウント制限 [2-84](#)

クラス マップ

一致基準の定義 [2-298](#)

作成 [2-59](#)

表示 [2-433](#)

グローバル コンフィギュレーション モード [1-2, 1-3](#)

け

検出メカニズム、原因 [2-151](#)

こ

候補スイッチ

「クラスタ」を参照

候補スイッチの拡張検出 [2-84](#)

コマンド スイッチ

「クラスタ」を参照

コンフィギュレーション ファイル

名前の指定 [2-44](#), [2-49](#)

パスワード回復のディセーブル化に関する考慮事項 [A-1](#)

さ

再認証

試行間隔時間 [2-135](#)

定期的な [2-132](#)

し

システム メッセージのログ [2-264](#)

システム メッセージのログ、フラッシュへのメッセージの保存 [2-265](#)

システム リソースのテンプレート [2-400](#)

ジャンボ フレーム

「MTU」を参照

柔軟な認証順序付け [2-27](#)

集約ポート ラーナー [2-359](#)

信頼されたポートの状態、QoS [2-337](#)

す

スイッチド ポート アナライザ

「SPAN」を参照

スイッチポート、表示 [2-482](#)

スタティック アクセス ポート、設定 [2-714](#)

スティッキ ラーニング、イネーブル化 [2-727](#)

スパニング ツリー プロトコル

「STP」を参照

せ

制御ポートの許可ステート [2-129](#)

制限 VLAN

「dot1x auth-fail vlan」を参照

製品 ID 情報、表示 [2-494](#)

セキュア ポート、制限 [2-729](#)

そ

送信元ポート、MVR [2-347](#)

即時脱退機能、MVR [2-347](#)

即時脱退処理 [2-226](#)

即時脱退処理、IPv6 [2-250](#)

ソフトウェア イメージ

アップグレード [2-6](#)

アップロード [2-12](#)

削除 [2-97](#)

ダウンロード [2-6](#)

ソフトウェア バージョン、表示 [2-626](#)

た

ダイナミック ARP インスペクション

ARP ACL

VLAN への適用 [2-180](#)

定義 [2-14](#)

パケットの許可 [2-363](#)

パケットの拒否 [2-99](#)

表示 [2-419](#)

VLAN ごとにイネーブル化 [2-190](#)

クリア

統計 [2-66](#)

ログ バッファ [2-65](#)

検証チェック [2-188](#)

信頼されるインターフェイス ステート [2-186](#)

着信 ARP パケットのレート制限 [2-182](#)

統計

クリア [2-66](#)

表示 [2-495](#)

表示

ARP ACL [2-419](#)

信頼状態とレート制限 [2-495](#)

設定と動作ステート [2-495](#)

統計 [2-495](#)

ログ バッファ [2-495](#)
 ログインされるパケットのタイプ [2-191](#)
 ログ バッファ
 クリア [2-65](#)
 設定 [2-184](#)
 表示 [2-495](#)
 ダイナミック アクセス ポート
 制限 [2-715](#)
 設定 [2-714](#)
 単一方向リンクの検出
 「UDLD」を参照

て

定義済みのコマンド モード [1-1](#)
 ディレクトリ、削除 [2-97](#)
 デュアルパーパス アップリンク ポート
 アクティブ メディアの表示 [2-489](#)
 設定可能なオプションの表示 [2-485](#)
 タイプの選択 [2-301](#)
 デュプレックス モードの自動ネゴシエーション [2-140](#)
 電源情報、表示 [2-468](#)
 転送結果、表示 [C-5](#)
 テンプレート、SDM [2-401](#)
 テンプレート、システム リソース [2-400](#)

と

統計、イーサネット グループ [2-399](#)
 特権 EXEC モード [1-2, 1-3](#)
 ドメイン名、VTP [2-779, 2-783](#)
 トランキング、VLAN モード [2-722](#)
 トランク、DTP をサポートしないデバイス [2-723](#)
 トランク ポート [2-722](#)
 トランク モード [2-722](#)

な

内部レジスタ、表示 [2-442, 2-451](#)

ね

ネイティブ VLAN [2-738](#)

は

ハードウェア ACL 統計情報 [2-415](#)
 パスワード、VTP [2-779, 2-783](#)
 パスワード回復メカニズム、イネーブル化およびディセーブル化 [2-402](#)
 バックアップ インターフェイス
 設定 [2-716](#)
 表示 [2-482](#)

ひ

非 IP トラフィック アクセス リスト [2-269](#)
 非 IP トラフィックの転送
 許可 [2-365](#)
 拒否 [2-101](#)
 非 IP プロトコル
 拒否 [2-101](#)
 転送 [2-365](#)
 非ネゴシエーション DTP メッセージング [2-725](#)
 標準範囲 VLAN [2-758, 2-764](#)

ふ

ファイル、削除 [2-97](#)
 ファイル名、VTP [2-779](#)
 ファン情報、表示 [2-468](#)
 ブートローダ
 アクセス [A-1](#)
 環境変数
 設定 [A-19](#)

- 設定の表示 [A-19](#)
 - 説明 [A-19](#)
 - 場所 [A-20](#)
 - リセット [A-23](#)
 - 起動
 - Cisco IOS イメージ [A-2](#)
 - ヘルパー イメージ [2-46](#)
 - システムのリセット [A-17](#)
 - ディレクトリ
 - 削除 [A-18](#)
 - 作成 [A-14](#)
 - リストの表示 [A-7](#)
 - 表示
 - 使用可能なコマンド [A-12](#)
 - バージョン [A-25](#)
 - メモリ ヒープ使用率 [A-13](#)
 - ファイル
 - コピー [A-5](#)
 - 削除 [A-6](#)
 - 内容の表示 [A-4, A-15, A-22](#)
 - 名前の変更 [A-16](#)
 - リストの表示 [A-7](#)
 - ファイル システム
 - 一貫性チェックの実行 [A-11](#)
 - 初期化、フラッシュ [A-9](#)
 - フォーマット [A-10](#)
 - プロンプト [A-1](#)
 - フォールバック プロファイル、表示 [2-478](#)
 - 負荷分散方式、EtherChannel [2-374](#)
 - 複数のインターフェイスの設定 [2-167](#)
 - 物理ポート ラーナー [2-359](#)
 - 不明なマルチキャスト トラフィック、回避 [2-720](#)
 - 不明なユニキャスト トラフィック、回避 [2-720](#)
 - プルーニング
 - VLAN [2-738](#)
 - VTP
 - イネーブル化 [2-779, 2-783](#)
 - インターフェイス情報の表示 [2-482](#)
 - プルーニング適格 VLAN リスト [2-739](#)
 - フレーム転送情報、表示 [C-5](#)
 - フロー制御パケットの受信 [2-163](#)
 - フロー制御パケットの送信 [2-163](#)
 - ブロードキャスト ストーム制御 [2-711](#)
-
- ## ほ
- ポート集約プロトコル
 - 「EtherChannel」を参照
 - ポート セキュリティ
 - イネーブル化 [2-727](#)
 - 違反エラーの回復 [2-157](#)
 - エージング [2-732](#)
 - デバッグ メッセージ、表示 [B-70](#)
 - ポート タイプ、MVR [2-347](#)
 - ポート、デバッグ [B-68](#)
 - ポート範囲、定義 [2-95](#)
 - ポートベース認証
 - AAA 方式リスト [2-3](#)
 - IEEE 802.1x AAA アカウンティング方式 [2-1](#)
 - IEEE 802.1x 準備状態のテスト [2-133](#)
 - IEEE 802.1x 対応ポートの再認証 [2-131](#)
 - IEEE 802.1x のイネーブル化
 - インターフェイス単位 [2-129](#)
 - グローバルに [2-104](#)
 - MAC 認証バイパス [2-124](#)
 - 違反モードの設定 [2-138](#)
 - インターフェイスの初期化 [2-123, 2-134](#)
 - オーセンティケータとしての PAE [2-128](#)
 - 許可ステータスの手動制御 [2-129](#)
 - ゲスト VLAN [2-119](#)
 - スイッチからクライアントへの再送信時間 [2-135](#)
 - スイッチから認証サーバへの再送信時間 [2-135](#)
 - スイッチとクライアント間のフレーム再送信回数 [2-126 to 2-127](#)
 - 設定可能な IEEE 802.1x パラメータのリセット [2-117](#)
 - 定期的な再認証
 - イネーブル化 [2-132](#)

試行間隔時間 **2-135**
 デバッグ メッセージ、表示 **B-8**
 認証交換に失敗したあとの待機時間 **2-135**
 ホスト モード **2-121**
 ポート、保護 **2-736**
 保護ポート、表示 **2-487**
 ホスト接続、ポート設定 **2-721**
 ポリシー マップ
 インターフェイスへの適用 **2-404, 2-408**
 階層 **2-373**
 作成 **2-372**
 トラフィックの分類
 DSCP 値または IP precedence 値の設定 **2-406**
 クラスの定義 **2-57**
 信頼状態の定義 **2-751**
 表示 **2-597**
 ポリサー
 単一クラス用 **2-368**
 表示 **2-565**
 複数のクラス **2-305, 2-370**
 ポリシング設定 DSCP マップ **2-311**
 ポリシング設定 DSCP マップ **2-311**

ま

マクロ
 インターフェイス範囲 **2-95, 2-167**
 作成 **2-296**
 説明の追加 **2-291**
 追加、global description **2-295**
 追跡 **2-292**
 適用 **2-292**
 パラメータ値の指定 **2-292**
 表示 **2-594**
 マップ
 QoS
 定義 **2-311**
 表示 **2-572**
 マルチキャスト VLAN、MVR **2-345**

マルチキャスト グループ、MVR **2-345**
 マルチキャスト グループ アドレス、MVR **2-347**
 マルチキャスト ストーム制御 **2-711**
 マルチキャスト ルータ学習方式 **2-228**
 マルチキャスト ルータ ポート、IPv6 **2-250**
 マルチキャスト ルータ ポート、設定 **2-228**

む

無効な GBIC
 エラー回復タイマー **2-157**
 エラー検出 **2-151**

め

メンバー スイッチ
 「クラスタ」を参照

も

モード、MVR **2-344**
 モード、コマンド **1-1**

ゆ

ユーザ EXEC モード **1-2, 1-3**
 ユニキャスト ストーム制御 **2-711**

ら

ライン コンフィギュレーション モード **1-2, 1-5**

り

リソース テンプレート、表示 **2-606**
 リモート スイッチド ポート アナライザ
 「RSPAN」を参照
 リンク フラップ

エラー回復タイマー [2-157](#)

エラー検出 [2-151](#)

る

ルートガード、スパニング ツリー用 [2-666](#)

ループガード、スパニング ツリー用 [2-666, 2-670](#)

ループバック エラー

回復タイマー [2-157](#)

検出 [2-151](#)

れ

レイヤ 2 traceroute

IP アドレス [2-749](#)

MAC アドレス [2-746](#)

レシーバー ポート、MVR [2-347](#)

ろ

論理インターフェイス [2-165](#)

