Review Draft -- Cisco Confidential

Cisco Nexus 6000 Series NX-OS Unicast Routing Command Reference

Cisco NX-OS Release 6.x

First Published: January 2013
Last Modified: 1/30/13

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

Text Part Number: OL-27917-01

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Cisco Nexus 6000 Series NX-OS Unicast Routing Command Reference
© 2012-2013 Cisco Systems, Inc. All rights reserved.

Review Draft -- Cisco Confidential

CONTENTS

Preface xix

Audience xix

Organization xix

Document Conventions xx

Related Documentation xxi

Documentation Feedback xxi

Obtaining Documentation and Submitting a Service Request xxi

xxii

BGP Commands 29

A Commands UCR-31

address-family ipv6 unicast UCR-32

address-family (BGP neighbor) UCR-33

address-family (BGP router) UCR-35

advertise-map (BGP) UCR-38

aggregate-address (BGP) UCR-40

B Commands UCR-43

bestpath (BGP) UCR-44

C Commands UCR-47

clear bgp UCR-48

clear bgp dampening UCR-49

clear bgp flap-statistics UCR-50

clear bgp policy statistics aggregate-address UCR-51

clear bgp policy statistics dampening UCR-52

clear bgp policy statistics neighbor UCR-53

clear bgp policy statistics redistribute UCR-54

clear ip bgp UCR-56

clear ip bgp dampening UCR-57

clear ip bgp flap-statistics UCR-58

client-to-client reflection UCR-59

Review Draft -- Cisco Confidential

confederation UCR-60

E Commands UCR-61

ebgp-multihop UCR-62

F Commands UCR-63

feature bgp UCR-64

H Commands UCR-65

hardware ip glean throttle UCR-66

hardware ip glean throttle maximum UCR-67

I Commands UCR-69

ip as-path access-list UCR-70

ip community-list UCR-72

ip extcommunity-list UCR-76

ip prefix-list UCR-78

ip prefix-list description UCR-80

L Commands UCR-81

local-as UCR-82

low-memory exempt UCR-83

M Commands UCR-85

mac-list UCR-86

match as-number UCR-87

match as-path UCR-88

match community UCR-90

match extcommunity UCR-92

match interface UCR-94

match ip address UCR-95

match ip multicast UCR-97

match ip next-hop prefix-list UCR-99

match ip route-source prefix-list UCR-101

match metric UCR-103

match mac-list UCR-105

match route-type UCR-107

match tag UCR-109

match vlan UCR-111

Review Draft -- Cisco Confidential

maxas-limit UCR-113
maximum-paths (BGP) UCR-114
maximum-prefix UCR-115

N Commands UCR-119
neighbor UCR-120
network UCR-123
nexthop route-map UCR-124
next-hop-self UCR-126
nexthop trigger-delay UCR-127

P Commands UCR-129
password (BGP) UCR-130

R Commands UCR-133
redistribute (BGP) UCR-134
remote-as UCR-136
restart (BGP) UCR-137
route-map UCR-138
route-reflector-client (BGP) UCR-142
router bgp UCR-143

S Commands UCR-147
send-community UCR-148
set as-path UCR-149
set comm-list delete UCR-151
set community UCR-153
set dampening UCR-155
set etxcommunity UCR-157
set extcomm-list delete UCR-159
set local-preference UCR-161
set metric UCR-163
set metric-type UCR-165
set origin UCR-167
set tag UCR-169
set weight UCR-170
shutdown (BGP) UCR-171
soft-reconfiguration inbound (BGP) UCR-172

Review Draft -- Cisco Confidential

suppress-inactive UCR-173

Show Commands UCR-175

show bgp UCR-176

show bgp community UCR-178

show bgp community-list UCR-179

show bgp extcommunity UCR-180

show bgp extcommunity-list UCR-181

show bgp neighbors UCR-182

show bgp sessions UCR-184

show bgp statistics UCR-185

show ip bgp UCR-187

show ip bgp all UCR-188

show ip bgp community UCR-191

show ip bgp community exact-match UCR-193

show ip bgp community-list UCR-194

show ip bgp dampening UCR-195

show ip bgp extcommunity UCR-196

show ip bgp extcommunity-list UCR-197

show ip bgp filter-list UCR-198

show ip bgp flap-statistics UCR-199

show ip bgp neighbors UCR-200

show ip bgp nexthop UCR-201

show ip bgp nexthop-database UCR-202

show ip bgp paths UCR-203

show ip bgp peer-policy UCR-204

show ip bgp peer-session UCR-205

show ip bgp peer-template UCR-206

show ip bgp prefix-list UCR-207

show ip bgp received-paths UCR-208

show ip bgp route-map UCR-209

show ip bgp summary UCR-210

show ip community-list UCR-211

show ip prefix-list UCR-212

show mac-list UCR-213

show vrf UCR-214

Review Draft -- Cisco Confidential

show vrf detail UCR-215
show vrf interface UCR-216

T Commands UCR-219
template (BGP) UCR-220

V Commands UCR-225
vrf UCR-226
vrf context UCR-229
vrf member UCR-230

EIGRP Commands 231

A Commands UCR-233
address-family (EIGRP) UCR-234
authentication key-chain (EIGRP) UCR-235
authentication mode (EIGRP) UCR-236
autonomous-system UCR-237

C Commands UCR-239
clear ip eigrp accounting UCR-240
clear ip eigrp neighbors UCR-241
clear ip eigrp redistribution UCR-243
clear ip eigrp traffic UCR-244

D Commands UCR-245
default-information originate (EIGRP) UCR-246
default-metric (EIGRP) UCR-247
distance (EIGRP) UCR-249

E Commands UCR-251
eigrp log-neighbor-changes UCR-252
eigrp log-neighbor-warnings UCR-253
eigrp router-id UCR-254
eigrp stub UCR-255

F Commands UCR-257
feature eigrp UCR-258
flush-routes (EIGRP) UCR-259

I Commands UCR-261
ip authentication key-chain eigrp UCR-262

Review Draft -- Cisco Confidential

ip authentication mode eigrp UCR-263
ip bandwidth eigrp UCR-264
ip bandwidth-percent eigrp UCR-265
ip delay eigrp UCR-266
ip distribute-list eigrp UCR-267
ip eigrp shutdown UCR-269
ip hello-interval eigrp UCR-270
ip hold-time eigrp UCR-271
ip next-hop-self eigrp UCR-273
ip offset-list eigrp UCR-274
ip passive-interface eigrp UCR-276
ip route UCR-277
ip router eigrp UCR-279
ip split-horizon eigrp UCR-280
ip summary-address eigrp UCR-281

L Commands UCR-283
log-adjacency-changes (EIGRP) UCR-284
log-neighbor-warnings UCR-285

M Commands UCR-287
maximum-paths (EIGRP) UCR-288
metric maximum-hops UCR-289
metric weights UCR-290

R Commands UCR-293
redistribute (EIGRP) UCR-294
redistribute maximum-prefix (EIGRP) UCR-296
restart eigrp (EIGRP) UCR-298
router eigrp UCR-299
router-id (EIGRP) UCR-300

S Commands UCR-301
shutdown (EIGRP) UCR-302
stub UCR-303

Show Commands UCR-305
show ip eigrp UCR-306

Review Draft -- Cisco Confidential

show ip eigrp accounting UCR-308
show ip eigrp interfaces UCR-310
show ip eigrp neighbors UCR-312
show ip eigrp route UCR-314
show ip eigrp route-map statistics UCR-316
show ip eigrp topology UCR-318
show ip eigrp traffic UCR-322
show running-config eigrp UCR-324

T Commands UCR-327
timers active-time UCR-328
timers nsf converge UCR-329
timers nsf route-hold UCR-330
timers nsf signal UCR-332

HSRP Commands 333

A Commands UCR-335
authentication (HSRP) UCR-336

D Commands UCR-339
delay minimum UCR-340

F Commands UCR-341
feature hsrp UCR-342

H Commands UCR-343
hsrp UCR-344
hsrp delay UCR-346

I Commands UCR-349
ip (HSRP) UCR-350
ipv6 (HSRP) UCR-352

P Commands UCR-355
preempt (HSRP) UCR-356
priority (HSRP) UCR-358

Show Commands UCR-361
show hsrp UCR-362
show hsrp delay UCR-364
show hsrp summary UCR-366

Review Draft -- Cisco Confidential

Layer 3 Interfaces Commands 369

C Commands UCR-371

clear ip arp UCR-372

clear ip interface statistics UCR-373

clear ipv6 icmp interface statistics UCR-374

clear ipv6 nd interface statistics UCR-375

clear ipv6 neighbor UCR-376

I Commands UCR-377

ip address UCR-378

ip arp UCR-380

ip arp gratuitous UCR-382

ip arp timeout UCR-383

ip directed-broadcast UCR-384

interface ethernet (Layer 3) UCR-386

ip local-proxy-arp UCR-388

interface loopback UCR-389

interface port-channel UCR-390

ip port-unreachable UCR-392

ip proxy-arp UCR-393

ip tcp path-mtu-discovery UCR-394

ip tcp synwait-time UCR-395

ip unreachables UCR-396

ipv6 nd UCR-397

N Commands UCR-399

no switchport UCR-400

R Commands UCR-401

routing-context vrf UCR-402

Show Commands UCR-403

show interface brief UCR-404

show interface ethernet UCR-408

show interface loopback UCR-411

show interface port-channel UCR-414

show ip arp UCR-416

Review Draft -- Cisco Confidential

show ip arp summary UCR-418
show ip client UCR-419
show ip interface UCR-420
show running-config arp UCR-422
show startup-config arp UCR-424
Object Tracking Commands 425
D Commands UCR-427
delay UCR-428
O Commands UCR-429
object UCR-430
Show Commands UCR-433
show track UCR-434
T Commands UCR-435
threshold percentage UCR-436
threshold weight UCR-437
track interface UCR-438
track ip route UCR-439
track list UCR-440
V Commands UCR-443
vrf member UCR-444
OSPF Commands 447
A Commands UCR-449
area authentication (OSPF) UCR-450
area default-cost (OSPF) UCR-452
area filter-list (OSPF) UCR-453
area nssa (OSPF) UCR-455
area range (OSPF) UCR-457
area stub (OSPF) UCR-459
area virtual-link (OSPF) UCR-460
authentication (OSPF virtual link) UCR-462
authentication-key (OSPF virtual link) UCR-464
auto-cost (OSPF) UCR-465

Review Draft -- Cisco Confidential

C Commands UCR-467

clear ip ospf neighbor UCR-468

clear ip ospf policy statistics UCR-470

clear ip ospf redistribution UCR-472

clear ip ospf statistics UCR-473

clear ip ospf traffic UCR-474

clear ip traffic UCR-475

D Commands UCR-477

dead-interval (OSPF virtual link) UCR-478

default-information originate (OSPF) UCR-480

default-metric (OSPF) UCR-482

distance (OSPF) UCR-484

F Commands UCR-485

feature ospf UCR-486

flush-routes (OSPF) UCR-487

H Commands UCR-489

hello-interval (OSPF virtual link) UCR-490

I Commands UCR-491

ip ospf authentication UCR-492

ip ospf authentication-key UCR-494

ip ospf cost UCR-496

ip ospf dead-interval UCR-497

ip ospf hello-interval UCR-498

ip ospf message-digest-key UCR-499

ip ospf mtu-ignore UCR-501

ip ospf network UCR-502

ip ospf passive-interface UCR-503

ip ospf priority UCR-504

ip ospf retransmit-interval UCR-505

ip ospf shutdown UCR-506

ip ospf transmit-delay UCR-507

ip router ospf area UCR-508

ip router ospf multi-area UCR-509

Review Draft -- Cisco Confidential

L Commands UCR-511

log-adjacency-changes (OSPF) UCR-512

M Commands UCR-513

max-metric router-lsa (OSPF) UCR-514

maximum-paths (OSPF) UCR-516

message-digest-key (OSPF virtual link) UCR-517

P Commands UCR-519

protocol shutdown (OSPF) UCR-520

R Commands UCR-521

redistribute (OSPF) UCR-522

redistribute maximum-prefix (OSPF) UCR-524

restart (OSPF) UCR-526

retransmit-interval (OSPF virtual link) UCR-527

rfc1583compatibility UCR-528

router ospf UCR-529

router-id (OSPF) UCR-530

S Commands UCR-531

set forwarding-address UCR-532

shutdown (OSPF) UCR-534

summary-address (OSPF) UCR-535

Show Commands UCR-537

show ip ospf UCR-538

show ip ospf border-routers UCR-541

show ip ospf database UCR-542

show ip ospf interface UCR-545

show ip ospf lsa-content-changed-list UCR-547

show ip ospf neighbors UCR-548

show ip ospf policy statistics area UCR-550

show ip ospf policy statistics redistribute UCR-552

show ip ospf request-list UCR-554

show ip ospf retransmission-list UCR-555

show ip ospf route UCR-556

show ip ospf statistics UCR-557

Review Draft -- Cisco Confidential

show ip ospf summary-address UCR-559
show ip ospf traffic UCR-560
show ip ospf virtual-links UCR-562
show ip traffic UCR-564
show running-config ospf UCR-566
show vrf UCR-568
show vrf detail UCR-569
show vrf interface UCR-570

T Commands UCR-573
timers lsa-arrival (OSPF) UCR-574
timers lsa-group-pacing (OSPF) UCR-575
timers throttle lsa (OSPF) UCR-577
timers throttle spf (OSPF) UCR-579
transmit-delay (OSPF virtual link) UCR-581

V Commands UCR-583
vrf UCR-584
vrf context UCR-587
vrf member UCR-588

RIP Commands 589

A Commands UCR-591
address-family (RIP) UCR-592

C Commands UCR-593
clear ip rip policy statistics redistribute UCR-594
clear ip rip statistics UCR-595

D Commands UCR-597
default-information originate (RIP) UCR-598
default-metric (RIP) UCR-599
distance (RIP) UCR-600

F Commands UCR-601
feature rip UCR-602

I Commands UCR-603
ip rip authentication key-chain UCR-604
ip rip authentication mode UCR-605

Review Draft -- Cisco Confidential

ip rip metric-offset UCR-606
ip rip offset-list UCR-607
ip rip passive-interface UCR-608
ip rip poison-reverse UCR-609
ip rip route-filter UCR-610
ip rip summary-address UCR-611
ip router rip UCR-612

M Commands UCR-613
maximum-paths (RIP) UCR-614

R Commands UCR-615
redistribute (RIP) UCR-616
restart (RIP) UCR-618
router rip UCR-619

Show Commands UCR-621
show ip rip UCR-622
show ip rip interface UCR-623
show ip rip neighbor UCR-624
show ip rip policy statistics UCR-625
show ip rip route UCR-627
show ip rip statistics UCR-628

T Commands UCR-629
timers basic UCR-630
Unicast RIB and FIB Commands 633

C Commands UCR-635
clear forwarding route UCR-636
clear forwarding inconsistency UCR-637
clear ip adjacency statistics UCR-638
clear ip route UCR-639
clear sockets statistics UCR-640

H Commands UCR-641
hardware profile ucast6 max-limit UCR-642

I Commands UCR-643
ip load-sharing address UCR-644

Review Draft -- Cisco Confidential

ip route UCR-645

Show Commands UCR-647

show forwarding UCR-648

show forwarding distribution UCR-650

show forwarding distribution multicast UCR-651

show forwarding distribution multicast client UCR-652

show forwarding distribution multicast outgoing-interface-list UCR-653

show forwarding distribution multicast route UCR-654

show forwarding inconsistency UCR-656

show forwarding multicast outgoing-interface-list UCR-657

show forwarding multicast route UCR-658

show ip adjacency UCR-660

show ip adjacency summary UCR-662

show ip fib UCR-663

show ip fib distribution UCR-664

show ip load-sharing UCR-665

show ip process UCR-666

show ip route UCR-667

show ip static-route UCR-668

show routing UCR-669

show routing memory estimate UCR-671

show routing hash UCR-672

show sockets client UCR-673

show sockets connection UCR-675

show sockets statistics UCR-677

T Commands UCR-679

test forwarding distribution perf UCR-680

test forwarding inconsistency UCR-681

VRRP Commands 683

A Commands UCR-685

address (VRRP) UCR-686

advertisement-interval (VRRP) UCR-688

authentication (VRRP) UCR-689

Review Draft -- Cisco Confidential

C Commands UCR-691

clear ip interface statistics UCR-692

clear vrrp UCR-693

F Commands UCR-695

feature vrrp UCR-696

P Commands UCR-697

preempt (VRRP) UCR-698

priority (VRRP) UCR-700

S Commands UCR-703

shutdown (VRRP) UCR-704

Show Commands UCR-705

show vrrp UCR-706

T Commands UCR-709

track (VRRP) UCR-710

track interface (VRRP) UCR-712

V Commands UCR-715

vrrp UCR-716

Review Draft -- Cisco Confidential

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 6000 Series NX-OS Unicast Routing Command Reference*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

- Audience, page xix
- This publication is for experienced users who configure and maintain Cisco NX-OS devices., page xix
- Organization, page xix
- Document Conventions, page xx
- Related Documentation, page xxi
- Obtaining Documentation and Submitting a Service Request, page xxi

Audience

This publication is for experienced users who configure and maintain Cisco NX-OS devices.

Organization

This document is organized as follows:

Chapter Title	Description
BGP Commands	Describes the Cisco NX-OS Border Gateway Protocol (BGP) commands.
EIGRP Commands	Describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands.
HSRP Commands	Describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) commands.
Layer 3 Interfaces Commands	Describes the Cisco NX-OS Layer 3 interfaces commands.
Object Tracking Commands	Describes the Cisco NX-OS object tracking commands.
OSPF Commands	Describes the Cisco NX-OS Open Shortest Path First (OSPF) commands.

Review Draft -- Cisco Confidential

Chapter Title	Description
RIP Commands	Describes the Cisco NX-OS Routing Information Protocol (RIP) commands.
Unicast RIB and FIB Commands	Describes the Cisco NX-OS unicast Routing Information Base (RIB) and the Forwarding Information Base (FIB) commands.
VRRP Commands	Describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader *be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Review Draft -- Cisco Confidential

Related Documentation

Documentation for the Cisco Nexus 6000 Series Switch is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

The documentation set is divided into the following categories:

Release Notes

The release notes are available at the follwing URL:

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

Installation and Upgrade Guides

The installation and upgrade guides are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html

Command References

The command references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_command_reference_list.html

Technical References

The technical references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html

Configuration Guides

The configuration guides are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html

Error and System Messages

The system message reference guide is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus6k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

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

Review Draft -- Cisco Confidential

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

<I_Italic>Review Draft -- Cisco Confidential

PART 1

BGP Commands

Review Draft -- Cisco Confidential

A Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with A.

Review Draft -- Cisco Confidential

address-family ipv6 unicast

To enter IPv6 unicast address family mode, use the **address-family ipv6 unicast** command.

address-family ipv6 unicast

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how enter IPv6 unicast address family mode:

```
switch# configure terminal
switch(config)# router ospfv 1234
switch(config-router)# neighbor 2001:DB8:0:1::55 remote-as 64496
switch(config-router-neighbor)# address-family ipv6 unicast
switch(config-router-af)# next-hop-self
```

Related Commands

Command	Description
area filter-list (OSPFv3)	Filters prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR).

Review Draft -- Cisco Confidential

address-family (BGP neighbor)

To enter the neighbor address family mode address-family mode and configure submode commands for the Border Gateway Protocol (BGP), use the **address-family** command. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

address-family ipv4{**multicast** | **unicast**}

no address-family ipv4 {**multicast** | **unicast**}

Syntax Description

ipv4	Specifies the IPv4 address family.
multicast	Specifies multicast address support.
unicast	Specifies unicast address support.

Command Default

This command has no default settings.

Command Modes

Neighbor configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **address-family** command to enter various address family configuration modes while configuring BGP routing. When you enter the **address-family** command from neighbor configuration mode, you enable the neighbor address family and enter the neighbor address family configuration mode. The prompt changes to `switch(config-router-neighbor-af)#`.

You must configure the address families if you are using route redistribution, load balancing, and other advanced features. IPv4 neighbor sessions support IPv4 unicast and multicast address families.

From the neighbor address family configuration mode, the following parameters are available:

Note This applies to IPv4 multicast or unicast

- **advertise-map**—Conditionally advertises selected BGP routes.
- **default-originate**—Configures a BGP routing process to distribute a default route.
- **exit**—Exits from the current command mode.
- **maximum-prefix**—Controls how many prefixes can be received from a neighbor.
- **no**—Negates a command or sets its defaults
- **route-reflector-client**—Configures the router as a BGP route reflector.
- **soft-reconfiguration inbound**—Configures the switch software to start storing BGP peer updates.
- **suppress-inactive**—Advertises only active routes to peer.

Review Draft -- Cisco Confidential

This command requires the LAN Enterprise Services license.

Examples

This example shows how to activate IPv4 multicast for neighbor 192.0.2.1 and place the device in neighbor address family configuration mode for the IPv4 multicast address family:

```
switch(config)# feature bgp
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1 remote-as 64496
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)
```

Related Commands

Command	Description
advertise-map	Configures BGP conditional advertisement.
default-originate (BGP)	Configures a BGP routing process to distribute a default route.
feature bgp	Enables BGP configuration.
maximum-prefix	Controls how many prefixes can be received from a neighbor.
route-reflector-client	Configures the router as a BGP route reflector.
soft-reconfiguration inbound	Configures the switch software to start storing BGP peer updates.
suppress-inactive	Advertises only active routes to peer.

Review Draft -- Cisco Confidential

address-family (BGP router)

To enter the address family mode or a virtual routing and forwarding (VRF) address-family mode and configure submode commands for the Border Gateway Protocol (BGP), use the **address-family** command. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

address-family ipv4 {**multicast** | **unicast**}

no address-family ipv4 {**multicast** | **unicast**}

Syntax Description

ipv4	Specifies the IPv4 address family.
multicast	Specifies multicast address support.
unicast	Specifies unicast address support.

Command Default

This command has no default settings.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **address-family** command to enter various address family configuration modes while configuring BGP routing. When you enter the **address-family** command from router configuration mode, you enable the address family and enter global address family configuration mode. The prompt changes to `switch(config-router-af)#`.

You must configure the address families if you are using route redistribution, address aggregation, load balancing, and other advanced features. IPv4 neighbor sessions support IPv4 unicast and multicast address families.

From the address family configuration mode, the following parameters are available:

Note This applies to IPv4 multicast or unicast.

- **aggregate-address**—Configures BGP aggregate prefixes. See the **aggregate-address** command for additional information.
- **client-to-client reflection**—Enables client-to-client route reflection. Route reflection allows a BGP speaker (route reflector) to advertise IBGP learned routes to certain IBGP peers. Use the **no** form of this command to disable client-to-client route reflection. Default: Enabled.

Review Draft -- Cisco Confidential

- **dampening** [*half-life* | **route-map** *name*]—Configures the route flap dampening. Optionally, you can set the time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The default half-life is 15 minutes. Range: 1 to 45. Default: Disabled.
- **default-metric** *metric*—Sets the default flap metric of redistributed routes. The **default-metric** command is used to set the metric value for routes redistributed into BGP with the **redistribute** command. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur. This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value. Range: 0 to 4294967295.

Note When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

- **distance** *ebgp-route ibgp-route local-route*—Configures a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. BGP does not use discard routes for next-hop resolution. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP. Range: 1 to 255. Default: EBGP—20, IBGP—200.

Caution Changing the administrative distance of internal BGP routes is considered dangerous and is not recommended. Improper configuration can introduce routing table inconsistencies and break routing.

- **exit**—Exits from the current command mode.
- **maximum-paths** [**ibgp**] *parallel-paths*—Configures the number of parallel paths to forward packets. The **maximum-paths ibgp** command is used to configure equal-cost or unequal-cost multipath load sharing for iBGP peering sessions. In order for a route to be installed as a multipath in the BGP routing table, the route cannot have a next hop that is the same as another route that is already installed. The BGP routing process will still advertise a best path to iBGP peers when iBGP multipath load sharing is configured. For equal-cost routes, the path from the neighbor with the lowest router ID is advertised as the best path. To configure equal-cost multipath load sharing, all path attributes must be the same. The path attributes include weight, local preference, autonomous system path (entire attribute and not just the length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance. The optional **ibgp** keyword allows you to configure multipath for the IBGP paths. To return to the default, use the **no** form of this command. The range is from 1 to 16.
- **network**—Configures an IP prefix to advertise. See the **network** command for additional information.
- **nexthop**—Configures next-hop address tracking events for BGP processes.
- **no**—Negates a command or sets its defaults.

Review Draft -- Cisco Confidential

- **redistribute**—Enables the redistribution of routes learned by other protocols into BGP. Redistribution is supported for both IPv4 routes. To disable the redistribution of routes learned by other protocols into BGP, use the **no** form of this command.
  - **direct route-map** *name*—Specifies directly connected routes.
  - **eigrp** *AS-num* **route-map** *name*—Specifies Enhanced Interior Gateway Protocol routes. Range: 1 to 65535.
  - **ospf** *src-protocol* **route-map** *name*—Specifies Open Shortest Path First (OSPF) routes.
  - **rip** *src-protocol* **route-map** *name*—Specifies Routing Information Protocol (RIP) routes.
  - **static route-map** *name*—Specifies static routes.
- **suppress-inactive**—Advertises only active routes to peer. See the **suppress-inactive** command for additional information.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to place the router in global address family configuration mode for the IPv4 unicast address family:

```
switch(config)# feature bgp
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)#
```

Related Commands

Command	Description
aggregate-address	Configures BGP summary addresses.
client-to-client reflection	Configures route reflection.
dampening	Configures route flap dampening.
default-metric (BGP)	Configures the default metric for routes redistributed into BGP.
distance (BGP)	Configures the administrative distance.
feature bgp	Enables BGP configuration.
maximum-paths (BGP)	Configures the maximum number of equal-cost paths.
network	Configures an IP prefix to advertise.
nexthop route-map	Configures route policy filtering for next hops.
nexthop trigger-delay	Configures the BGP delay for triggering next-hop calculations.
redistribute (BGP)	Configures route redistribution for BGP.
suppress-inactive	Advertises active routes to a BGP peer.
timers (BGP)	Configures the BGP timers.

Review Draft -- Cisco Confidential

advertise-map (BGP)

To configure Border Gateway Protocol (BGP) conditional advertisement, use the **advertise-map** command. To remove BGP conditional advertisement, use the **no** form of this command.

advertise-map *adv-map* {**exist-map** *exist-rmap* | **non-exist-map** *nonexist-rmap*}

no advertise-map *adv-map* {**exist-map** *exist-rmap* | **non-exist-map** *nonexist-rmap*}

Syntax Description

adv-map	Route map with match statements that the route must pass before BGP passes the route to the next route map. The *adv-map* is a case-sensitive, alphanumeric string up to 63 characters.
exist-map *exist-rmap*	Specifies a route map with match statements for a prefix list. A prefix in the BGP table must match a prefix in the prefix list before BGP will advertise the route. The *exist-rmap* is a case-sensitive, alphanumeric string up to 63 characters.
non-exist-map *nonexist-rmap*	Specifies a route map with match statements for a prefix list. A prefix in the BGP table must not match a prefix in the prefix list before BGP will advertise the route. The *nonexist-rmap* is a case-sensitive, alphanumeric string up to 63 characters.

Command Default

None

Command Modes

BGP neighbor address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **advertise-map** command to conditionally advertise selected routes. The routes or prefixes that BGP conditionally advertises are defined in two route maps, the *adv-map* and an *exist-map* or *nonexist-map*. The e*xist-map* or *nonexist-map* specifies the prefix that the BGP tracks. The *adv-map* specifies the prefix that BGP advertises to the specified neighbor when the condition is met.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure BGP conditional advertisement:

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.2 remote-as 65537
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# advertise-map advertise exist-map exist
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# exit
switch(config)# route-map advertise
switch(config-route-map)# match as-path pathList
```

Review Draft -- Cisco Confidential

```
switch(config-route-map)# exit
switch(config)# route-map exit
switch(config-route-map)# match ip address prefix-list plist
switch(config-route-map)# exit
switch(config)# ip prefix-list plist permit 209.165.201.0/27
switch(config)#
```

Related Commands

Command	Description
feature bgp	Enables BGP.
neighbor	Configures a BGP peer.
show ip bgp	Displays BGP configuration information.

Review Draft -- Cisco Confidential

aggregate-address (BGP)

To create a summary address in a Border Gateway Protocol (BGP) routing table, use the **aggregate-address** command. To remove the summary address, use the **no** form of this command.

aggregate-address *address/length* [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

no aggregate-address *address/mask-length* [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

Syntax Description

address/length	Aggregate IPv4 address and mask length. Valid value for *length* is 1 to 32.
advertise-map *map-name*	(Optional) Specifies the name of the route map used to select attribute information from specific routes.
as-set	(Optional) Generates the autonomous system set path information and community information from the contributing paths.
attribute-map *map-name*	(Optional) Specifies the name of the route map used to set the attribute information for specific routes. The *map-name* is an alphanumeric string up to 63 characters.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map *map-name*	(Optional) Specifies the name of the route map used to conditionally filter more specific routes. The *map-name* is an alphanumeric string up to 63 characters.

Command Default

The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the **as-set** keyword is specified.

Command Modes

Address family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can implement aggregate routing in BGP either by redistributing an aggregate route into BGP, or by using the conditional aggregate routing feature.

The **aggregate-address** command without keywords creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available that fall within the specified range. (A longer prefix which matches the aggregate must exist in the RIB.) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Review Draft -- Cisco Confidential

The **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

The **summary-only** keyword not only creates the aggregate route (for example, 192.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

The **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the match clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

The **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists match clauses are supported.

The **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

This command requires the LAN Enterprise Services license.

Examples

AS-Set Example

This example shows how to create an aggregate BGP address in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
switch(config)# router bgp 64496
switch(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set
```

Summary-Only Example

This example shows how to create an aggregate BGP address in address family configuration mode and apply it to the multicast database (SAFI) under the IP Version 4 address family. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 multicast
switch(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

Conditional Aggregation Example

This example shows how to create a route map called MAP-ONE to match on an as-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
switch(config)# ip as-path access-list 1 deny ^1234_
switch(config)# ip as-path access-list 1 permit .*
switch(config)# !
```

Review Draft -- Cisco Confidential

```
switch(config)# route-map MAP-ONE
switch(config-route-map)# match ip as-path 1
switch(config-route-map)# exit
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4
switch(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map
MAP-ONE
switch(config-router-af)# end
```

Related Commands

Command	Description
route-map	Creates a route map.

Review Draft -- Cisco Confidential

B Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with B.

Review Draft -- Cisco Confidential

bestpath (BGP)

To change the default best-path selection algorithm, use the **bestpath** command. To return the Border Gateway Protocol (BGP) routing process to the default operation, use the **no** form of this command.

bestpath {**always-compare-med** | **compare-routerid** | {**med** {**missing-as-worst** | **non-deterministic**}}

no bestpath {**always-compare-med** | **compare-routerid** | {**med** {**missing-as-worst** | **non-deterministic**}}

Syntax Description

always-compare-med	Compares the Multi-Exit Discriminator (MED) on paths from a different autonomous system (AS).
compare-routerid	Configures a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path.
med missing-as-worst	Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable.
med non-deterministic	Specifies that the best-MED path among paths is not picked from the same AS.

Command Default

The default settings are as follows:
med missing-as-worst: A value of 0 is assigned to the missing MED
med non-deterministic: Disabled

Command Modes

Router BGP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, ensure that BGP is enabled on the switch by using the **feature bgp** command.

To enable the comparison of the MED for paths from neighbors in different autonomous systems, use the **bgp always-compare-med** command.

This command requires the LAN Enterprise Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to change the default best-path selection algorithm to compare the MED on paths from different autonomous systems:

```
switch(config)# router bgp 64496
switch(config-router)# bestpath always-compare-med
switch(config-router)#
```

Related Commands

Command	Description
feature bgp	Enables BGP globally.
show ip bgp	Displays information about BGP routes.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with C.

Review Draft -- Cisco Confidential

clear bgp

To clear Border Gateway Protocol (BGP) routes from the BGP table, use the **clear bgp** command.

clear bgp {**ipv4** {**multicast** | **unicast**} | **all**} {*neighbor* | * | *as-number* | **peer-template** *name* | *prefix*} [**vrf** *vrf-name*]

Syntax Description

ipv4	Clears the BGP information for the IPv4 address family.
multicast	Clears BGP information for the multicast address family.
unicast	Clears BGP information for the unicast address family.
all	Clears the BGP information for all address families.
neighbor	Network address. The format is A.B.C.D for IPv4.
*	Clears all neighbors.
as-number	Autonomous system number. The range is from 1 to 65535.
peer-template *name*	Specifies a BGP peer template. The name can be any case-sensitive, alphanumeric string up to 63 characters.
prefix	Prefix from the selected address family. The format is A.B.C.D/length for IPv4.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) context name or all VRF instances. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear all BGP entries:

```
switch# clear bgp all *
```

Review Draft -- Cisco Confidential

clear bgp dampening

To clear Border Gateway Protocol (BGP) route flap dampening information, use the **clear bgp dampening** command.

clear bgp {**ipv4** {**unicast** | **multicast**} | **all**} **dampening** [*neighbor* | *prefix*] [**vrf** *vrf-name* | **all** | **default** | **management**]

Syntax Description

ipv4	Clears BGP information for the IPv4 address family.
unicast	Clears BGP information for the unicast address family.
multicast	Clears BGP information for the multicast address family.
all	Clears BGP information for all address families.
neighbor	(Optional) Neighbor from the selected address family. The format is A.B.C.D for IPv4.
prefix	(Optional) Prefix from the selected address family. The format is A.B.C.D/length for IPv4.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Clears BGP information from all VRFs.
default	(Optional) Clears BGP information from the default VRF.
management	(Optional) Clears BGP information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear BGP route flap dampening information:

```
switch# clear bgp all dampening
```

Review Draft -- Cisco Confidential

clear bgp flap-statistics

To clear Border Gateway Protocol (BGP) route flap statistics, use the **clear bgp flap-statistics** command.

clear bgp {**ipv4** {**multicast** | **unicast**} | **all**} **flap-statistics** [*neighbor* | *prefix*] [**vrf** *vrf-name* | **all** | **default** | **management**]

Syntax Description

ipv4	Clears BGP information for the IPv4 address family.
unicast	Clears BGP information for the unicast address family.
multicast	Clears BGP information for the multicast address family.
all	Clears BGP information for all address families.
neighbor	(Optional) Neighbor from the selected address family. The format is *A.B.C.D* for IPv4.
prefix	(Optional) Prefix from the selected address family. The format is *A.B.C.D/length* for IPv4.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Clears BGP information from all VRFs.
default	(Optional) Clears BGP information from the default VRF.
management	(Optional) Clears BGP information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear BGP route flap statistics:

```
switch# clear bgp ipv4 multicast flap-statistics
```

Review Draft -- Cisco Confidential

clear bgp policy statistics aggregate-address

To clear policy statistics for the Border Gateway Protocol (BGP) topology table, use the **clear bgp policy statistics aggregate address** command.

clear bgp policy statistics aggregate-address *prefix* {**advertise-map** | **suppress-map**}

Syntax Description

prefix	Summary address. The format is *x.x.x.x* or *x.x.x.x/length*. The range is from 1 to 32.
advertise-map	Clears policy statistics for the advertise policy.
suppress-map	Clears policy statistics for the suppress policy.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear policy statistics for an aggregate address:

```
switch# clear bgp policy statistics aggregate-address 192.0.2.0/8
```

Related Commands

Command	Description
show bgp policy statistics	Displays BGP policy statistics.

Review Draft -- Cisco Confidential

clear bgp policy statistics dampening

To clear policy statistics for the Border Gateway Protocol (BGP) dampening, use the **clear bgp policy statistics dampening** command.

clear bgp policy statistics dampening

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear policy statistics for dampening:

```
switch# clear bgp policy statistics dampening
```

Related Commands

Command	Description
show bgp policy statistics	Displays BGP policy statistics.

Review Draft -- Cisco Confidential

clear bgp policy statistics neighbor

To clear policy statistics for the Border Gateway Protocol (BGP) neighbor, use the **clear bgp policy statistics neighbor** command.

clear bgp policy statistics neighbor *prefix* [**default-originate** | {**filter-list** | **prefix-list** | **route-map**} {**in** | **out**}]

Syntax Description

prefix	Neighbor address. The format is x.x.x.x.
default-originate	(Optional) Clears policy statistics for the default originate policy.
filter-list	(Optional) Clears policy statistics for the neighbor filter list.
prefix-list	(Optional) Clears policy statistics for the neighbor prefix list.
route-map	(Optional) Clears policy statistics for the neighbor route map.
in	(Optional) Clears inbound policy statistics.
out	(Optional) Clears outbound policy statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear policy statistics for an aggregate address:

```
switch# clear bgp policy statistics neighbor 192.0.2.1 filter-list in
```

Related Commands

Command	Description
show bgp policy statistics	Displays BGP policy statistics.

Review Draft -- Cisco Confidential

clear bgp policy statistics redistribute

To clear policy statistics for the Border Gateway Protocol (BGP) topology table, use the **clear bgp policy statistics redistribute** command.

clear bgp policy statistics redistribute {**direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

direct	Clears policy statistics for directly connected routes only.
eigrp	Clears policy statistics for Enhanced Interior Gateway Routing Protocol (EIGRP).
ospf	Clears policy statistics for the Open Shortest Path First (OSPF) protocol.
rip	Clears policy statistics for the Routing Information Protocol (RIP).
static	Clears policy statistics for IP static routes.
id	For the **eigrp** keyword, an EIGRP instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string. For the **ospf** keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.
all	(Optional) Specifies the “all” VRF instance.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear policy statistics for RIP:

```
switch# clear bgp policy statistics redistribute rip 201
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show bgp policy statistics	Displays BGP policy statistics.

Review Draft -- Cisco Confidential

clear ip bgp

To clear Border Gateway Protocol (BGP) routes from the BGP table, use the **clear ip bgp** command.

clear ip bgp {**ipv4** {**unicast** | **multicast**} | **all**} {*neighbor* | * | *as-number* | **peer-template** *name* | *prefix*} [**vrf** *vrf-name* | **all** | **default** | **management**]

Syntax Description

ipv4	(Optional) Clears BGP information for the IPv4 address family.
unicast	Clears BGP information for the unicast address family.
multicast	Clears BGP information for the multicast address family.
all	Clears the BGP information for all address families.
neighbor	Network address. The format is A.B.C.D for IPv4.
*	Clears all BGP routes.
as-number	Autonomous system (AS) number. The range is from 1 to 65535.
peer-template *name*	Specifies a BGP peer template. The name can be any case-sensitive, alphanumeric string up to 63 characters.
prefix	Prefix from the selected address family. The format is A.B.C.D/length for IPv4.
vrf *vrf-name*	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Clears the BGP information from all VRF entries.
default	(Optional) Clears the BGP information from the default VRF.
management	(Optional) Clears the BGP information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear all BGP entries for the IPv4 address family:

```
switch# clear ip bgp *
```

Review Draft -- Cisco Confidential

clear ip bgp dampening

To clear Border Gateway Protocol (BGP) route flap dampening information, use the **clear ip bgp dampening** command.

clear ip bgp [**ipv4** {**unicast** | **multicast**} | **all**] **dampening** [*neighbor* | *prefix*] [**vrf** *vrf-name* | **all** | **default** | **management**]

Syntax Description

ipv4	(Optional) Clears BGP information for the IPv4 address family.
unicast	(Optional) Clears BGP information for the unicast address family.
multicast	(Optional) Clears BGP information for the multicast address family.
all	(Optional) Clears the BGP information for all address families.
neighbor	(Optional) Neighbor from the selected address family. The format is A.B.C.D for IPv4.
prefix	(Optional) Prefix from the selected address family. The format is A.B.C.D/length for IPv4.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Clears the BGP information from all VRF entries.
default	(Optional) Clears the BGP information from the default VRF.
management	(Optional) Clears the BGP information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Command History

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear BGP route flap dampening information:

```
switch# clear ip bgp dampening
```

Review Draft -- Cisco Confidential

clear ip bgp flap-statistics

To clear Border Gateway Protocol (BGP) route flap statistics, use the **clear ip bgp flap-statistics** command.

clear ip bgp flap-statistics [*neighbor* | *prefix*] [**vrf** *vrf-name* | **all** | **default** | **management**]

Syntax Description

neighbor	(Optional) Neighbor from the selected address family. The format is A.B.C.D for IPv4.
prefix	(Optional) Prefix from the selected address family. The format is A.B.C.D/length for IPv4.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Clears the BGP information from all VRF entries.
default	(Optional) Clears the BGP information from the default VRF.
management	(Optional) Clears the BGP information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to clear BGP route flap statistics:

```
switch# clear ip bgp flap-statistics
```

Review Draft -- Cisco Confidential

client-to-client reflection

To enable or restore route reflection from a Border Gateway Protocol (BGP) route reflector to clients, use the **client-to-client reflection** command. To disable client-to-client route reflection, use the **no** form of this command.

client-to-client reflection

no client-to-client reflection

Syntax Description

This command has no arguments or keywords.

Command Default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the **no client-to-client reflection** command to disable client-to-client reflection.

Examples

This example shows how to configure a router as a route reflector:

```
switch(config)# router bgp 50000
switch(config-router)# address-family ipv4 multicast
switch(config-router-af)# client-to-client reflection
switch(config-router-af)#
```

Related Commands

Command	Description
address-family (BGP router)	Places the router in address family configuration mode for configuring routing sessions that use standard IPv4 address prefixes.
show ip bgp	Displays entries in the BGP routing table.

Review Draft -- Cisco Confidential

confederation

To configure the confederation parameters for the Border Gateway Protocol (BGP), use the **confederation** command.

confederation {**identifier** | **peers**} *as-number*

Syntax Description

identifier	Sets the routing domain confederation autonomous system (AS) number.
peers	Sets the peer AS numbers for a BGP confederation.
as-number	Autonomous system number. The AS number can be a 16-bit integer or a 32-bit integer in the form of <higher 16-bit decimal number>.<lower 16-bit decimal number>.

Command Default

None

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure the confederation identifier:

```
switch# configure terminal
switch(config)# router bgp 65536.33
switch(config-router)# confederation identifier 65536.33
```

Related Commands

Command	Description
show bgp	Displays information about BGP.

Review Draft -- Cisco Confidential

E Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with E.

Review Draft -- Cisco Confidential

ebgp-multihop

To configure the exterior Border Gateway Protocol (eBGP) time-to-live (TTL) value to support eBGP multihop, use the **ebgp-multihop** command. To return to the default setting, use the **no** form of this command.

ebgp-multihop *ttl-value*

no ebgp-multihop *ttl-value*

Syntax Description

ttl-value	TTL value for eBGP multihop. The range is from 2 to 255. You must manually reset the BGP sessions after using this command.

Command Default

None

Command Modes

BGP neighbor configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ebgp-multihop** command to configure the eBGP time-to-live (TTL) value to support eBGP multihop. In some situations, an eBGP peer is not directly connected to another eBGP peer and requires multiple hops to reach the remote eBGP peer. You can configure the eBGP TTL value for a neighbor session to allow these multihop sessions.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure the eBGP multihop value:

```
switch(config)# router bgp 1.1
switch(config-router)# neighbor 192.0.2.1 remote-as 1.2
switch(config-route-neighbor) ebgp-multihop 2
```

Related Commands

Command	Description
feature bgp	Enables the BGP feature.

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with F.

Review Draft -- Cisco Confidential

feature bgp

To enable the Border Gateway Protocol (BGP), use the **feature bgp** command. To disable BGP, use the **no** form of this command.

feature bgp

no feature bgp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the BGP feature before you can configure BGP.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to enable a BGP configuration:

```
switch# configure terminal
switch(config)# feature bgp
switch(config)#
```

This example shows how to disable the BGP feature:

```
switch# configure terminal
switch(config)# no feature bgp
switch(config)#
```

Related Commands

Command	Description
router bgp	Creates a BGP instance.
show bgp	Displays BGP configuration information.
show feature	Displays the status of features on a switch.

Review Draft -- Cisco Confidential

H Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with H.

Review Draft -- Cisco Confidential

hardware ip glean throttle

To enable Address Resolution Protocol (ARP) throttling, use the **hardware ip glean throttle** command. To return to the default setting, use the **no** form of this command.

hardware ip glean throttle

no hardware ip glean throttle

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Note We recommend that you configure the IP glean throttle feature by using the **hardware ip glean throttle** command to filter the unnecessary glean packets that are sent to the supervisor for ARP resolution for the next hops that are not reachable or do not exist. IP glean throttling boosts software performance and helps to manage traffic more efficiently.

This command does not require a license.

Examples

This example shows how to enable ARP throttling:

```
switch(config)# hardware ip glean throttle
switch(config)#
```

Related Commands

Command	Description
show hardware proxy layer-3 detail	Displays Layer-3 proxy detail information.

Review Draft -- Cisco Confidential

hardware ip glean throttle maximum

To limit the maximum number of drop adjacencies that will be installed in the Forwarding Information Base (FIB), use the **hardware ip glean throttle maximum** command. If **no** form is used, default limits will be applied.

hardware ip glean throttle maximum *count*

no hardware ip glean throttle maximum *count*

Syntax Description

count	Maximum count. The range is from 0 to 2147483647.

Defaults

The default value for count is 1000. The minimum value is 0 and the maximum value is 32767 entries

Command Modes

Global configuration

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If the maximum number of entries are exceeded, the packets for which ARP is not resolved continue to be processed in the software instead of getting dropped in the hardware.

This command does not require a license.

Examples

This example shows how to limit the maximum number of drop adjacencies that are installed in the FIB:

```
switch(config)# hardware ip glean throttle maximum 2134
switch(config)#
```

Related Commands

Command	Description
show hardware proxy layer-3 detail	Displays Layer-3 proxy detail information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with I.

Review Draft -- Cisco Confidential

ip as-path access-list

To configure an access-list filter for Border Gateway Protocol (BGP) autonomous system (AS) numbers, use the **ip as-path access-list** command. To remove the filter, use the **no** form of this command.

ip as-path access-list *name* {**deny** | **permit**} *regexp*

no ip as-path access-list *name* {**deny** | **permit**} *regexp*

Syntax Description

name	AS path access list name. The name can be any alphanumeric string up to 63 characters.
deny	Rejects packets with AS numbers that match the *regexp* argument.
permit	Allows packets with AS numbers that match the *regexp* argument.
regexp	Regular expression to match BGP AS paths. See the *Cisco Nexus 6000 Series NX-OS Fundamentals Configuration Guide, Release 6.0* at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/fundamentals/621_n1_1/Cisco_Nexus_6000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6_2_1_N1_1_chapter4.html#con_1237003

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip as-path access-list** command to configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the permit or deny condition applies. The autonomous system path should not contain the local autonomous system number.

Examples

This example shows how to configure an AS path filter for BGP to permit AS numbers 55:33 and 20:01 and apply it to a BGP peer for inbound filtering:

```
switch# configure terminal
switch(config)# ip as-path access-list filter1 permit 55:33,20:01
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# filter-list filter1 in
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
filter-list	Assigns an AS path filter to a BGP peer.
show ip as-path access-list	Displays information about IP AS path access lists.

Review Draft -- Cisco Confidential

ip community-list

To create a community list entry, use the **ip community-list** command. To remove the entry, use the **no** form of this command.

ip community-list standard *list-name* {**deny** | **permit**} {*aa*:*nn* | **internet** | **local-AS** | **no-advertise** | **no-export**}

no ip community-list standard *list-name*

ip community-list expanded *list-name* {**deny** | **permit**} *regexp*

no ip community-list expanded *list-name*

Syntax Description

standard *list-name*	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
aa:*nn*	Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space. You can pick more than one of these optional community keywords.
internet	Specifies the Internet community. Routes with this community are advertised to all peers (internal and external). You can pick more than one of these optional community keywords.
no-export	Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers. You can pick more than one of these optional community keywords.
local-AS	Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised external peers or to other subautonomous systems within a confederation. You can pick more than one of these optional community keywords.
no-advertise	Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external). You can pick more than one of these optional community keywords.

Review Draft -- Cisco Confidential

expanded *list-name*	Configures a named expanded community list.
regexp	Regular expression that is used to specify a pattern to match against an input string. See the *Cisco Nexus 6000 Series NX-OS Fundamentals Configuration Guide, Release 6.0* at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/fundamentals/621_n1_1/Cisco_Nexus_6000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6_2_1_N1_1_chapter4.html#con_1237003 **Note** Regular expressions can be used with expanded community lists only.

Command Default

Community exchange is not enabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip community-list** command is used to configure BGP community filtering. BGP community values are configured as a 4-byte number. The first two bytes represent the autonomous system number, and the last two bytes represent a user-defined network number. BGP community attribute exchange between BGP peers is enabled when the **send-community** command is configured for the specified neighbor. The BGP community attribute is defined in RFC 1997 and RFC 1998.

BGP community exchange is not enabled by default. Use the **send-community** command in BGP neighbor fix-family configuration mode to enable a BGP community attribute exchange between BGP peers.

The Internet community is applied to all routes or prefixes by default until any other community value is configured with this command or the **set community** command.

Once you configure a permit value to match a given set of communities, the community list defaults to an implicit deny for all other community values. Use the **internet** community to apply an implicit permit to the community list.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. You can pick more than one of the optional community keywords.A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the communities that exceed the limit are not processed or saved to the running configuration file.

You can configure up to 32 communities.

Review Draft -- Cisco Confidential

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is the longest construct is first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.

Community List Processing

When multiple values are configured in the same community list statement, a logical AND condition is created. All community values must match to satisfy an AND condition. When multiple values are configured in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

This example shows how to configure a standard community list where the routes with this community are advertised to all peers (internal and external):

```
switch(config)# ip community-list standard test1 permit internet
switch(config)#
```

This example shows how to configure a logical AND condition; all community values must match in order for the list to be processed:

```
switch(config)# ip community-list standard test1 permit 65534:40 65412:60 no-export
switch(config)#
```

In the above example, a standard community list is configured that permits routes from the following:

- Network 40 in autonomous system 65534 and from network 60 in autonomous system 65412.
- Peers in the same autonomous system or from subautonomous system peers in the same confederation.

This example shows how to configure a standard community list that denies routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
switch(config)# ip community-list standard test2 deny 65534:40 65412:60
```

This example shows how to configure a named standard community list that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
switch(config)# ip community-list standard RED permit local-AS

switch(config)# ip community-list standard RED permit 40000:20
switch(config)#
```

This example shows how to configure an expanded community list that denies routes that carry communities from any private autonomous system:

```
switch(config)# ip community-list expanded 500 deny
_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
switch(config)#
```

This example shows how to configure a named expanded community list that denies routes from network 1 through 99 in autonomous system 50000:

```
switch(config)# ip community-list list expanded BLUE deny 50000:[0-9][0-9]_
```

Review Draft -- Cisco Confidential

```
switch(config)#
```

Related Commands

Command	Description
feature bgp	Enables BGP.
match community	Matches a community in a route map.
send-community	Configures BGP to propagate community attributes to BGP peers.
set community	Sets a community in a route map.

Review Draft -- Cisco Confidential

ip extcommunity-list

To create an extended community list entry, use the **ip extcommunity-list** command. To remove the entry, use the **no** form of this command.

ip extcommunity-list standard *list-name* {**deny** | **permit**} **generic** {**transitive** | **nontransitive**} *aa4*:*nn*

no ip extcommunity-list standard generic {**transitive** | **nontransitive**} *list-name*

ip extcommunity-list expanded *list-name* {**deny** | **permit**} **generic** {**transitive** | **nontransitive**} *regexp*

no ip extcommunity-list expanded generic {**transitive** | **nontransitive**} *list-name*

Syntax Description

standard *list-name*	Configures a named standard extended community list.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
generic	Specifies the generic specific extended community type.
transitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
nontransitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
aa4:*nn*	Autonomous system number and network number. This value is configured with a 4-byte AS number and a 2-byte network number separated by a colon. The 4-byte AS number range is from 1 to 4294967295 in plaintext notation, or from 1.0 to 56636.65535 in AS.dot notation. You can enter a single community or multiple communities, each separated by a space.
expanded *list-name*	Configures a named expanded extended community list.
regexp	Regular expression that is used to specify a pattern to match against an input string. See the *Cisco Nexus 6000 Series NX-OS Fundamentals Configuration Guide, Release 6.0* at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/fundamentals/621_n1_1/Cisco_Nexus_6000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6_2_1_N1_1_chapter4.html#con_1237003 **Note** Regular expressions can be used with expanded extended community lists only.

Command Default

Community exchange is not enabled by default.

Command Modes

Global configuration mode

Review Draft -- Cisco Confidential

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip extcommunity-list** command to configure extended community filtering for BGP. Extended community values are configured as a 6-byte number. The first four bytes represent the autonomous system number, and the last two bytes represent a user-defined network number. The BGP generic specific community attribute is defined in draft-ietf-idr-as4octet-extcomm-generic-subtype-00.txt.

BGP extended community exchange is not enabled by default. Use the **send-extcommunity** command in BGP neighbor fix-family configuration mode to enable extended community attribute exchange between BGP peers.

Once you configure a permit value to match a given set of extended communities, the extended community list defaults to an implicit deny for all other extended community values.

Standard Extended Community Lists

Use standard extended community lists to configure specific extended community numbers. You can configure a maximum of 16 extended communities in a standard extended community list.

Expanded Extended Community Lists

Use expanded extended community lists to filter communities using a regular expression. Use regular expressions to configure patterns to match community attributes. The order for matching using the * or + character is the longest construct is first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.

Community List Processing

When you configure multiple values in the same extended community list statement, a logical AND condition is created. All extended community values must match to satisfy the AND condition. When you configure multiple values in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

This example shows how to configure a standard generic specific extended community list that permits routes from network 40 in autonomous system 1.65534 and from network 60 in autonomous system 1.65412:

```
switch(config)# ip extcommunity-list standard test1 permit generic transitive 1.65534:40
1.65412:60
switch(config)#
```

All community values must match in order for the list to be processed.

Related Commands

Command	Description
feature bgp	Enables BGP.
match extcommunity	Matches an extended community in a route map.
send-community	Configures BGP to propagate community attributes to BGP peers.
set extcommunity	Sets an extended community in a route map.

Review Draft -- Cisco Confidential

ip prefix-list

To create a prefix list to match IP packets or routes against, use the **ip prefix-list** command. To remove the prefix-list, use the **no** form of this command.

ip prefix-list *name* [**seq** *number*] {**permit** | **deny**} *prefix* [**eq** *length* | [**ge** *length*] [**le** *length*]]

no ip prefix-list *name* [**seq** *number*] {**permit** | **deny**} *prefix* [**eq** *length* | [**ge** *length*] [**le** *length*]]

Syntax Description

name	IP prefix list name. The name can be any alphanumeric string up to 63 characters.
seq *number*	(Optional) Specifies the number to order entries in the prefix list. The range is from 1 to 4294967294.
permit	Allows routes or IP packets that match the prefix list.
deny	Rejects routes or IP packets that match the prefix list.
prefix	IP prefix in A.B.C.D/length format.
eq *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.
ge *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.
le *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip prefix-list** command to configure IP prefix filtering. Configure prefix lists with **permit** or **deny** keywords to either permit or deny the prefix based on the matching condition. A prefix list consists of an IP address and a bit mask. The bit mask is entered as a number from 1 to 32. An implicit deny is applied to traffic that does not match any prefix-list entry.

You can configure prefix lists to match an exact prefix length or a prefix range. Use the **ge** and **le** keywords to specify a range of the prefix lengths to match, which provides a more flexible configuration. If you do not configure a sequence number, Cisco NX-OS applies a default sequence number of 5 to the prefix list and subsequent prefix list entries are incremented by 5 (for example, 5, 10, 15, and so on). If you configure a sequence number for the first prefix list entry but not subsequent entries, then Cisco NX-OS increments the subsequent entries by 5 (for example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and so on). You can suppress default sequence numbers by entering the **no** form of this command with the **seq** keyword.

Cisco NX-OS evaluates prefix lists that start with the lowest sequence number and continue down the list until a match is made. Once a match is made, the **permit** or **deny** statement is applied to that network and the rest of the list is not evaluated.

Review Draft -- Cisco Confidential

Tip For the best performance of your network, you should configure the most frequently processed prefix list statements with the lowest sequence numbers. The **seq** *number* keyword and argument can be used for resequencing.

The prefix list is applied to inbound or outbound updates for specific peer by entering the **prefix-list** command in neighbor address-family mode. Prefix list information and counters are displayed in the output of the **show ip prefix-list** command. Prefix-list counters can be reset by entering the **clear ip prefix-list** command.

Examples

This example shows how to configure a prefix list and apply it to a Border Gateway Protocol (BGP) peer:

```
switch# configure terminal
switch(config)# ip prefix-list allowprefix 10 permit 192.0.2.0 eq 24
switch(config)# ip prefix-list allowprefix 20 permit 209.165.201.0 eq 27
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
switch(config-router-neighbor-af)#
```

Related Commands

Command	Description
clear ip prefix-list	Clears counters for IP prefix lists.
prefix-list	Applies a prefix list to BGP peer.
show ip prefix-list	Displays information about IP prefix lists.

Review Draft -- Cisco Confidential

ip prefix-list description

To configure a description string for an IP prefix list, use the **ip prefix-list description** command. To revert to default, use the **no** form of this command.

ip prefix-list *name* **description** *string*

no ip prefix-list *name* **description**

Syntax Description

name	Name of the prefix list. The name can be any alphanumeric string up to 63 characters.
string	Descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to configure a description for an IP prefix list:

```
switch# configure terminal
switch(config)# ip prefix-list test1 description "this is a test"
switch(config)#
```

Related Commands

Command	Description
show ip prefix-list	Displays information about IPv4 prefix lists.

Review Draft -- Cisco Confidential

L Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with L.

Review Draft -- Cisco Confidential

local-as

To configure the Border Gateway Protocol (BGP) local autonomous system (AS) number, use the **local-as** command.

local-as *as-number*

Syntax Description

as-number	(Optional) Autonomous system number. The AS number can be a 16-bit integer or a 32-bit integer in the form of <higher 16-bit decimal number>.<lower 16-bit decimal number>.

Command Default

None

Command Modes

Router VRF mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure the local AS number for BGP:

```
switch# configure terminal
switch(config)# router bgp 65536.33
switch(config-router)# vrf red
switch(config-router-vrf)# local-as 65536.33
```

Related Commands

Command	Description
show bgp	Displays information about BGP.

Review Draft -- Cisco Confidential

low-memory exempt

To exempt a Border Gateway Protocol (BGP) neighbor from a low-memory shutdown, use the **low-memory exempt** command. To make a BGP neighbor eligible for a low-memory shutdown, use the **no** form of this command.

low-memory exempt

no low-memory exempt

Syntax Description

This command has no arguments or keywords.

Command Default

Some eBGP peers shut down for severe memory alerts.

Command Modes

Neighbor configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to exempt a neighbor from low-memory shutdown:

```
switch(config)# router bgp 1.0
switch(config-router)# neighbor 192.0.2.0/24 remote-as 1.5
switch(config-router-af)# low-memory exempt
```

Related Commands

Command	Description
feature bgp	Enables BGP.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

M Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with M.

Review Draft -- Cisco Confidential

mac-list

To filter based on a MAC address, use the **mac-list** command. To remove the MAC list entry, use the **no** form of this command.

mac-list *name* [**seq** *number*] {**permit** | **deny**} *mac-address* [*mac-mask*]

no mac-list *name* [**seq** *number*] {**permit** | **deny**} *mac-address* [*mac-mask*]

Syntax Description

name	MAC list name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
seq *number*	(Optional) Creates an entry in the MAC list. The *seq* range is from 1 to 4294967294.
permit	Allows the packet or route that matches a MAC address in the MAC list.
deny	Blocks the packet or route that matches a MAC address in the MAC list.
mac-address	MAC address to filter against.
mac-mask	(Optional) Portion of the MAC address to match against, in MAC address format.

Command Default

No match values are defined.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can match against the MAC list in a route map.

Examples

This example shows how to create the Red MAC list:

```
switch(config)# mac-list Red seq 1 permit 0022.5579.a4c1 ffff.ffff.0000
```

Related Commands

Command	Description
match mac-list	Matches a MAC address in a MAC list.
show mac-list	Displays information about a MAC list.

Review Draft -- Cisco Confidential

match as-number

To match to a Border Gateway Protocol (BGP) autonomous system (AS) number, use the **match as-number** command. To remove an AS number list entry, use the **no** form of this command.

match as-number {*number* [,*number*...] | **as-path-access-list** *name* [...*name*]}

no match as-number {*number* [,*number*...] | **as-path-access-list** *name* [...*name*]}]

Syntax Description

number	AS number. The range is from 1 to 65535.
...*number*	(Optional) AS number. The range is from 1 to 65535.
as-path-access-list *name*	Specifies an AS-path access list to match AS numbers against. The name can be any alphanumeric string up to 63 characters.
...*name*	(Optional) AS-path access list. The name can be any alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Command History

Usage Guidelines

Use the **match as-number** command to provide a list of AS numbers or an AS-path access list using a regular expression. BGP uses this match criteria to determine which BGP peers to create a BGP session with.

Use the route map to specify a range of AS numbers whose peers can establish a session with the local BGP through prefix peering. Cisco NX-OS ignores any other **match** commands if the **match as-number** command is present in the route map.

Examples

This example shows how to configure a list of AS numbers:

```
switch(config)# route-map IGP2BGP
switch(config-route-map)# match as-number 64496, 64498-64510
```

Related Commands

Command	Description
ip as-path access-list	Creates an AS-path list.
neighbor	Configures BGP peers.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

Review Draft -- Cisco Confidential

match as-path

To match a Border Gateway Protocol (BGP) autonomous system (AS) path access list, use the **match as-path** command. To remove a path list entry, use the **no** form of this command.

match as-path *name* [*...name*]

no match as-path *name* [*...name*]

Syntax Description

name	Autonomous system path access list. The name can be any alphanumeric string up to 63 characters.
...name	(Optional) Autonomous system path access list. You can configure up to 32 access list names.

Command Default

No path lists are defined.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The values set by the **match as-path** command overrides global values.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route-map section with an explicit match specified.

Examples

This example sets the autonomous system path to match BGP autonomous system path access list 20:

```
switch(config)# route-map IGP2BGP
switch(config-route-map)# match as-path 20
switch(config-route-map)#
```

Related Commands

Command	Description
match community	Matches a BGP community.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match route-type	Redistributes routes of the specified type.

Review Draft -- Cisco Confidential

Command	Description
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set comm-list	Automatically computes the tag value in a route map configuration.
set community	Sets BGP community list (for deletion).
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match community

To match a Border Gateway Protocol (BGP) community, use the **match community** command. To remove the **match community** command from the configuration file and restore the system to its default condition where the software removes the BGP community list entry, use the **no** form of this command.

match community *name* [*...name*] [**exact-match**]

no match community *name* [*...name*] [**exact-match**]

Syntax Description

name	One or more community list names. The name can be any alphanumeric string up to 63 characters. You can configure a maximum of 32 community lists.
exact-match	(Optional) Indicates that an exact match is required. All of the communities and only those communities specified must be present.

Command Default

No community list is matched by the route map.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

A route map can have several parts. Any route that does not match at least one **match** command that is related to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route-map section with an explicit match specified.

Matching that is based on the community list number is one of the types of **match** commands applicable to BGP.

Examples

This example shows how to match two BGP communities:

```
switch(config)# route-map test2
switch(config-route-map)# match community bgpLow bgpHigh
```

This example shows that the routes that match community list 1 have the weight set to 200. Any route that has the standard community 109 only has the weight set to 200.

```
switch(config)# ip community-list standard bgpLow permit 109
switch(config)# route-map set_weight
switch(config-route-map)# match community bgpLow exact-match
switch(config-route-map)# set weight 200
```

This example shows the routes that match the community list 500. Any route that has expanded community 1 have the weight set to 150.

Review Draft -- Cisco Confidential

```
switch(config)# ip community-list expanded 500 permit [0-9]*
switch(config)# route-map MAP_NAME permit 10
switch(config-route-map)# match community 500
switch(config-route-map)# set weight 150
```

Related Commands

Command	Description
ip community-list	Creates a community list for BGP and controls access to it.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match extcommunity

To match a Border Gateway Protocol (BGP) extended community in a route map, use the **match extcommunity** command. To remove the match from the route map, use the **no** form of this command.

match extcommunity *name* [*...name*] [**exact-match**]

no match extommunity *name* [*...name*] [**exact-match**]

Syntax Description]

name	One or more extended community list names. The name can be any alphanumeric string up to 63 characters. You can configure a maximum of 32 community lists.
exact-match	(Optional) Indicates that an exact match is required. All of the communities and only those extended communities specified must be present.

Command Default

No community list is matched by the route map.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

A route map can have several parts. Any route that does not match at least one **match** command in the route map is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route-map section with an explicit match specified.

Matching that is based on the extended community list number is one of the types of **match** commands applicable to BGP.

Examples

This example shows how to match two BGP extended community lists:

```
switch(config)# route-map test2
switch(config-route-map)# match extcommunity bgpLocal bgpRemote
```

This example shows that the routes that match the extended community list bgpLocal change from nontransitive to transitive:

```
switch(config)# ip extcommunity-list standard bgpLocal permit generic nontransitive 1.9
switch(config)# route-map deletCommunity
switch(config-route-map)# match extcommunity bgpLocal exact-match
switch(config-route-map)# set extcommunity generic transitive 1.9
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
ip extcommunity-list	Creates a community list for BGP and controls access to it.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
send-community	Configures BGP to propagate community attributes to BGP peers.
set extcommunity	Sets an extended community in a route map.

Review Draft -- Cisco Confidential

match interface

To match an interface in a route map, use the **match interface** command. To remove the match, use the **no** form of this command.

match interface {*interface-type number* [, *interface-type number*...]}

no match interface {*interface-type number* [, *interface-type number*...]}

Syntax Description

interface-type	Interface type. Use **?** to see a list of supported interfaces.
number	(Optional) Interface number. Use **?** to see the range.

Command Default

None

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Route next-hop addresses that are reached by one of the interfaces result in a match for the route map.

A route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route-map section with an explicit match specified.

Examples

This example shows how to configure a list of interfaces:

```
switch(config)# route-map test1
switch(config-route-map)# match interface ethernet 2/1, ethernet 4/3
```

Related Commands

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

Review Draft -- Cisco Confidential

match ip address

To distribute any routes that have a destination IP network number address that is permitted by a standard access list, an expanded access list, or a prefix list, use the **match ip address** command. To remove the **match ip address** entry, use the **no** form of this command.

match ip address {**prefix-list** *prefix-list-name* [*prefix-list-name...*]}

no match ip address {**prefix-list** *prefix-list-name* [*prefix-list-name...*]}

Syntax Description

prefix-list *prefix-list-name...*	Distributes routes based on a prefix list. The prefix list name can be any alphanumeric string up to 63 characters. The ellipsis indicates that multiple values can be entered, up to 32 prefix lists.

Command Default

No prefix lists are specified.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *prefix-list-name* argument.

Like matches in the same route map subblock are filtered with “or” semantics. If any one match clause is matched in the entire route map subblock, this match is treated as a successful match. Dissimilar match clauses are filtered with “and” semantics, so dissimilar matches are filtered logically. If the first set of conditions is not met, the second match clause is filtered. This process continues until a match occurs or there are no more match clauses.

Use route maps to redistribute routes.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Review Draft -- Cisco Confidential

When you are passing routes through a route map, a route map can have several sections that contain specific **match** clauses. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route map section with an explicit match specified.

Examples

This example shows how to match routes that have addresses specified by an access list test:

```
switch(config)# interface ethernet 2/10
switch(config-if)# no switchport
switch(config-if)# exit
switch(config)# route-map chicago
switch(config-route-map)# match ip address test
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match ip multicast

To configure the IPv4 multicast features for the route-map matching, use the **match ip multicast** command. To remove the match, use the **no** form of this command.

match ip multicast {**group** *address/length* | **source** *address/length* | **rp** *address/length* [**rp-type asm**]}

no match ip multicast

Syntax Description

group *address/length*	Specifies the group address and the length of the network mask in bits in this format: *A.B.C.D/length*. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32. You can configure group, source, and rp options.
source *address/length*	Specifies the source address and the length of the network mask in bits in this format: *A.B.C.D/length*. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32. You can configure group, source, and rp options.
rp *address/length*	*S*pecifies the IPv4 rendezvous prefix (RP) and the length of the IPv4 prefix mask in bits in this format: *A.B.C.D/length*. The network number can be any valid IPv4 address or prefix. The bit mask can be a number from 0 to 32. You can configure group, source, and rp options.
rp-type	(Optional) Specifies the multicast rendezvous point type.
asm	(Optional) Specifies the any-source multicast (ASM) rendezvous point type.

Command Default

None

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **match ip multicast** command is the only **match** command that is evaluated in the route map. You can specify the group prefix, group range, and source prefix to filter messages with the **match ip multicast** command.

Use the **route-map** command to enter route-map configuration mode. Once you enter the **route-map** command, the prompt changes to the following:

```
switch(config-route-map)#
```

Once you enter route-map configuration mode, you can enter the **match ip multicast** command.

Review Draft -- Cisco Confidential

You can configure both group and rp options.

Examples

This example shows how to specify the group IPv4 prefix and the length of the IPv4 prefix for the neighbors to match:

```
switch(config)# route-map blueberry
switch(config-route-map)# match ip multicast group 192.0.0.0/19
switch(config-route-map)#
```

This example shows how to specify both the group IPv4 prefix and the rendezvous point of the IPv4 prefix for the neighbors to match:

```
switch(config)# route-map raspberry
switch(config-route-map)# match ip multicast group 192.0.0.0/19 rp 209.165.201.0/27
switch(config-route-map)#
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match ip next-hop prefix-list

To redistribute any IPv4 routes that have a next-hop router address passed by one of the access lists specified, use the **match ip next-hop prefix-list** command. To remove the next hop entry, use the **no** form of this command.

match ip next-hop prefix-list *prefix-list-name* [*...prefix-list-name*]

no match ip next-hop prefix-list *prefix-list-name* [*...prefix-list-name*]

Syntax Description

prefix-list-name	Number or name of a prefix list. It can be any alphanumeric string up to 63 characters. The ellipsis indicates that multiple values can be entered, up to 32 prefix lists.

Command Default

Routes are distributed freely, without being required to match a next hop address.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Command History

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *prefix-list-name* argument.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route map section with an explicit match specified.

Examples

This example shows how to distributes routes that have a next-hop router address passed by the prefix list test:

Review Draft -- Cisco Confidential

```
switch(config)# route-map blue
switch(config-route-map)# match ip next-hop prefix-list test
switch(config-route-map)#
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match route-type	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set communit	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match ip route-source prefix-list

To redistribute IPv4 routes that have been advertised by routers and access servers at the address specified by the access lists, use the **match ip route-source prefix-list** command. To remove the route-source entry, use the **no** form of this command.

match ip route-source prefix-list *prefix-list-name* [*...prefix-list-name*]

no match ip route-source prefix-list *prefix-list-name* [*...prefix-list-name*]

Syntax Description

prefix-list-name	Number or name of a prefix list. It can be any alphanumeric string up to 63 characters. The ellipsis indicates that multiple values can be entered, up to 32 prefix lists.

Command Default

No filtering on route source.

Command Modes

Route-map mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *prefix-list-name* argument.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify only some data, you must configure second route map section with an explicit match specified.

There are situations in which the next hop and source router address of the route are not the same.

Review Draft -- Cisco Confidential

Examples

This example shows how to distribute routes that have been advertised by routers and access servers at the addresses specified by access lists 5 and 80:

```
switch(config)# route-map blue
switch(config-route-map)#  match ip route-source prefix-list 5 80
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match metric

To redistribute routes in the routing table that match the routing metric value, use the **match metric** command. To remove the tag entry, use the **no** form of this command.

match metric *metric-value* [**+-** *deviation-number*] [*...metric-value* [**+-** *deviation-number*]]

no match metric *metric-value* [**+-** *deviation-number*] [*...metric-value* [**+-** *deviation-number*]]

Syntax Description

metric-value	Internal route metric. The range is from 1 to 4,294,967,295.
+ -	Specifies a standard deviation range of the metric. The router matches any metric that falls inclusively in that range.
deviation-number	(Optional) Standard deviation number that offsets the number configured for the *metric-value* argument. The *deviation-number* argument can be any number. There is no default.

Command Default

No match values are defined.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To redistribute routes with the specified metric, use the **match metric** command in route-map configuration mode. To remove the entry for the redistributed route from the routing table, use the no form of this command.

You can specify one or more metrics (or) range of metrics using the *deviation-number* argument. At least one of the specified metrics must match for the command to pass.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the arguments.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Review Draft -- Cisco Confidential

A route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure second route map section with an explicit match specified.

Examples

This example shows how to redistribute routes stored in the routing table with a metric of 5:

```
switch(config)# route-map blueberry
switch(config-route-map)# match metric 5
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match mac-list

To redistribute routes in the routing table that match a MAC address in the MAC list, use the **match mac-list** command. To remove the tag entry, use the **no** form of this command.

match mac-list *listname*

no match mac-list *listname*

Syntax Description

listname	MAC list name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

No match values are defined.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route map section with an explicit match specified.

Examples

This example shows how to redistribute routes stored in the routing table that match entries in the Red MAC list:

```
switch# configure terminal
switch(config)# route-map blueberry
switch(config-route-map)# match mac-list Red
switch(config-route-map)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match route-type

To redistribute routes of the specified type, use the **match route-type** command. To remove the route type entry, use the **no** form of this command.

match route-type {**external** | **internal** | **local** | **nssa-external** | **type-1** | **type-2**}

no match route-type {**external** | **internal** | **local** | **nssa-external** | **type-1** | **type-2**}

Syntax Description

external	Specifies the external route (Border Gateway Protocol [BGP], Enhanced Interior Gateway Routing Protocol [EIGRP], and Open Shortest Path First [OSPF] type 1/2). You can specify more than one keyword.
internal	Specifies the internal route (including the OSPF intra/inter area). You can specify more than one keyword.
local	Specifies the locally generated route. You can specify more than one keyword.
nssa-external	Specifies the nssa-external route (OSPF type 1/2). You can specify more than one keyword.
type-1	Specifies the OSPF external type 1 route. You can specify more than one keyword.
type-2	Specifies the OSPF external type 2 route. You can specify more than one keyword.

Command Default

Disabled

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Review Draft -- Cisco Confidential

A route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route map section with an explicit match specified.

You can specify more than one keyword.

Examples

This example shows how to redistribute internal routes:

```
switch(config)# route-map blueberry
switch(config-route-map)# match route-type internal
```

This example shows how to redistribute internal routes and type-1 OSPF routes:

```
switch(config)# route-map blueberry
switch(config-route-map)# match route-type internal type-1
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match tag

To redistribute routes in the routing table that match the specified tags, use the **match tag** command. To remove the tag entry, use the **no** form of this command.

match tag *tag-value* [*...tag-value*]

no match tag *tag-value* [*...tag-value*]

Syntax Description

tag-value	List of one or more route tag values. Each can be an integer from 0 to 4,294,967,295. You can configure up to 32 tags.

Command Default

No match tag values are defined.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *tag-value* argument.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route map section with an explicit match specified.

Examples

This example shows how to redistribute routes stored in the routing table with tag 5:

```
switch(config)# route-map blueberry
switch(config-route-map)# match tag 5
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

match vlan

To filter routes with the specified VLAN, use the **match vlan** command. To remove the entry for the redistributed route from the routing table, use the **no** form of this command.

match vlan *vlan-range*

no match vlan *vlan-range*

Syntax Description

vlan-range	Range of VLAN that this command matches against. The range is from 1 to 4094.

Command Default

No match VLAN values are defined.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To filter routes with the specified VLAN, use the **match vlan** command You can specify one or more VLANs (or) range of VLANs. At least one of the specified VLANs must match for the command to pass. The command matches any VLAN that falls inclusive in the range.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route map section with an explicit match specified

Examples

This example shows how to redistribute routes that match VLANs 5 to 10:

```
switch(config)# route-map blueberry
switch(config-route-map)# match vlan 5-10
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

maxas-limit

To configure the external Border Gateway Protocol (eBGP) to discard routes that have a high number of autonomous system (AS) numbers in the AS-path attribute, use the **maxas-limit** command. To revert to the default, use the **no** form of this command.

maxas-limit [*number*]

no maxas-limit

Syntax Description

number	(Optional) Maximum number of AS numbers allowed in the AS-path attribute. The range is from 1 to 2000.

Command Default

No limit

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to set the maximum number of AS numbers to 50:

```
switch(config)# router bgp 64496
switch(config-router)# maxas-limit 50
switch(config-router)#
```

Related Commands

Command	Description
feature bgp	Enables the BGP feature.
router bgp	Creates a BGP instance.

Review Draft -- Cisco Confidential

maximum-paths (BGP)

To control the maximum number of parallel routes that the Border Gateway Protocol (BGP) can support, use the **maximum-paths** command. To restore the default number of parallel routes, use the **no** form of this command.

maximum-paths [**ibgp**] *number-paths*

no maximum-paths [**ibgp**] *number-paths*

Syntax Description

ibgp	(Optional) Configures the maximum interior BGP (iBGP) paths.
number-paths	Maximum number of parallel routes that an IP routing protocol installs in a routing table. The range is from 1 to 16.

Command Default

8 paths

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to allow a maximum of 16 paths to a destination for a BGP routing process:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# maximum-paths 16
switch(config-router)#
```

Related Commands

Command	Description
feature bgp	Enables the BGP feature on the router.
router bgp	Enables BGP.

Review Draft -- Cisco Confidential

maximum-prefix

To control how many prefixes can be received from a neighbor, use the **maximum-prefix** command. To disable this function, use the **no** form of this command.

maximum-prefix *maximum* [**threshold**] [**restart** *restart-interval*] [**warning-only**]

no maximum-prefix

Syntax Description

maximum	Maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router. Range: 1 to 300000.
threshold	(Optional) Specifies the percentage of the maximum-prefix limit at which the router starts to generate a warning message. Range: 1 to 100. Default: 75.
restart *interval*	(Optional) Specifies the time interval (in minutes) that a peering session is reestablished. Range: 1 to 65535.
warning-only	(Optional) Allows the router to generate a syslog message when the maximum-prefix limit is exceeded, instead of terminating the peering session.

Command Default

This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. If you do not configure the restart interval, a disabled session stays down after the maximum-prefix limit is exceeded.

Command Modes

Peer template configuration mode

BGP router configuration mode

BGP neighbor address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The number of prefixes that can be configured is limited only by the available system resources on a router.

The **maximum-prefix** command allows you to configure a maximum number of prefixes that a Border Gateway Protocol (BGP) routing process accepts from the specified peer. This feature provides a mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, BGP disables the peering session (by default). If you configure the restart interval, BGP automatically reestablishes the peering session at the configured time interval. If you do not configure the restart interval and a peering

Review Draft -- Cisco Confidential

session is terminated because the maximum prefix limit has been exceed, the peering session is not reestablished until you enter the **clear ip bgp** command. If the **warning-only** keyword is configured, BGP sends only a log message and continues to peer with the sender.

There is no default limit on the number of prefixes that can be configured with this command. Limitations on the number of prefixes that can be configured are determined by the amount of available system resources.

Examples

This example shows how to set the maximum prefixes that are accepted from the 192.168.1.1 neighbor to 1000:

```
switch(config)# router bgp 64496
switch(config-router)# network 192.168.0.0
switch(config-router)# maximum-prefix 1000
switch(config-router)#
```

This example shows how to set the maximum number of prefixes that are accepted from the 192.168.2.2 neighbor to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
switch(config)# router bgp 64496
switch(config-router)# network 192.168.0.0
switch(config-router)# maximum-prefix 5000 50
switch(config-router)#
```

This example shows how to set the maximum number of prefixes that are accepted from the 192.168.3.3 neighbor to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
switch(config)# router bgp 64496
switch(config-router)# network 192.168.0.0
switch(config-router)# maximum-prefix 2000 restart 30
switch(config-router)#
```

This example shows how to set the warning messages that are displayed when the maximum-prefix limit (500) for the 192.168.4.4 neighbor is exceeded:

```
switch(config)# router bgp 64496
switch(config-router)# network 192.168.0.0
switch(config-router)# maximum-prefix 500 warning-only
switch(config-router)#
```

This example shows how to set the maximum number of prefixes that are accepted from the 192.168.1.3 neighbor to 1500.

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.168.1.3 remote-as 64497
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)# maximum-prefix 1500
switch(config-router-neighbor-af)#
```

Related Commands

Command	Description
address-family (BGP neighbor)	Enters BGP neighbor address-family configuration mode.
neighbor	Configures a BGP neighbor.

Review Draft -- Cisco Confidential

Command	Description
network	Configures an IP prefix to advertise.
show ip bgp	Displays BGP configuration information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

N Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with N.

Review Draft -- Cisco Confidential

neighbor

To configure a Border Gateway Protocol (BGP) neighbor (router or VRF) and enter the neighbor configuration mode, use the **neighbor** command. To remove an entry, use the **no** form of this command.

neighbor {*ip-addr* | *ip-prefix/length*} [**remote-as** {*as-num*[.*as-num*] | **route-map** *name*}

no neighbor {*ip-addr* | *ip-prefix/length*} [**remote-as** {*as-num*[.*as-num*] | **route-map** *name*}]

Syntax Description

ip-addr	IP address of the neighbor in this format: A.B.C.D.
ip-prefix/length	IP prefix and the length of the IP prefix. The format is x.x.x.x/*length*. The *length* range is from 1 to 32.
remote-as	(Optional) Specifies the autonomous system (AS) number of the neighbor.
as-num	Number of an AS that identifies the router to other BGP routers and tags the routing information passed along. The range is from 1 to 65535.
.*as-num*	(Optional) Number of an AS that identifies the router to other BGP routers and tags the routing information passed along. The range is from 1 to 65535.
route-map *name*	(Optional) Specifies a route map that matches the BGP peer AS number against a list of AS numbers or a regular expression. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Neighbor address-family configuration mode

Router BGP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

From the BGP neighbor configuration mode, you can perform the following actions:

- **address-family**—Configures an address-family (router, neighbor, VRF). See the **address-family (BGP)** command for information.
- **description** *description*—Describes the neighbor. You can enter up to 80 characters including spaces.
- **disable-connected-check**—Disables the connection verification for the directly connected peer. Use the **disable-connected-check** command to disable a check for an exterior Border Gateway Protocol (eBGP) peer that is directly connected to the local router. BGP triggers a connection check

Review Draft -- Cisco Confidential

automatically for all eBGP peers that are known to be a single hop away, unless you disable this check with the **disable-connected-check** command. BGP does not bring up sessions if the check fails. BGP considers an EBGP peer as a single hop away if the eBGP peer does does not have the **ebgp-multihop** command configured (that is, the time-to-live (TTL) value is one).

This command is ignored if the **route-map** keyword is used in the **neighbor** command.

- **dont-capability-negotiate**—Turns off the negotiate capability with this neighbor.
- **dynamic-capability**—Enables the dynamic capability.
- **ebgp-multihop**—Accepts and attempts BGP connections to external peers that reside on networks that are not directly connected. This command is ignored if the **route-map** keyword is used in the **neighbor** command.

Note You should enter this command under the guidance of Cisco technical support staff only.

- **exit**—Exits from the current command mode.
- **inherit peer-session** *session-name*—Configures a peer to inherit the configuration from another peer-session template. To remove an inherit statement from a peer-session template, use the **no** form of this command.
- **no**—Negates a command or sets its defaults.
- **transport connection-mode passive**—Allows a passive connection setup only. To remove the restriction, use the **no** form of this command.
- **remove-private-as**—Removes the private AS number from the outbound updates.
- **shutdown**—Administratively shuts down this neighbor.
- **timers** *keepalive-time*—Configures keepalive and hold timers in seconds. The range is from 0 to 3600. The default is 60.
- **update-source** {**ethernet** *mod/port* | **loopback** *virtual-interface* | **port-channel** *number*[**.***sub-interface*]}—Specifies the source of the BGP session and updates. The range for *virtual-interface* is from 0 to 1023. The range for *number* is from 0 to 4096. The range for *sub-interface* is from 1 to 4093.

  The Cisco NX-OS software allows BGP sessions to use any operational interface for TCP connections when you enter the **update-source** command in neighbor configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure a single-hop eBGP peering session between two BGP peers that are reachable on the same network segment through a local loopback interfaces on each router:

BGP Peer 1

```
switch(config)# interface loopback 1
switch(config-if)# ip address 10.0.0.100 255.255.255
switch(config-if)# exit
switch(config)# router bgp 64497
switch(config-router)# neighbor 192.168.0.200 remote-as 64496
switch(config-router-neighbor)# update-source loopback 2
switch(config-router-neighbor)# disable-connected-check
switch(config-router-neighbor)#
```

Review Draft -- Cisco Confidential

BGP Peer 2

```
switch(config)# interface loopback 2
switch(config-if)# ip address 192.168.0.200 255.255.255
switch(config-if)# exit
switch(config)# router bgp 64496
switch(config-router)# neighbor 10.0.0.100 remote-as 64497
switch(config-router-neighbor)# update-source loopback 1
switch(config-router-neighbor)# disable-connected-check
switch(config-router-neighbor)#
```

This example shows how to source BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 172.16.0.0 remote-as 64496
switch(config-router-neighbor)# update-source Loopback0
switch(config-router-neighbor)#
```

Related Commands

Command	Description
feature bgp	Enables BGP on the router.
route-map	Creates a route map.

Review Draft -- Cisco Confidential

network

To configure an IP prefix to advertise, use the **network** command. To remove the IP prefix to advertise, use the **no** form of this command.

network *ip-addr* | *ip-prefix/length* **mask** *mask-num* [**route-map** *name*]

no network *ip-network* | *ip-prefix/length* **mask** *mask-num* [**route-map** *name*]

Syntax Description

ip-addr	IP network address to advertise; use the following format: A.B.C.D.
ip-prefix/length	IP prefix and the length of the IP prefix. Use the following format: A.B.C.D/length.
mask *mask-num*	Configures the mask of the IP prefix to advertise in dotted 4-octet format.
route-map *name*	(Optional) Specifies the name of the route map to modify attributes.

Command Default

None

Command Modes

Neighbor address-family configuration mode

Router BGP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The IP prefix to advertise is considered as a best path and advertisement to peers only if a route of equal or more specificity is present in the routing table.

Examples

This example shows how to configure an IP prefix to advertise:

```
switch(config-router-af)# network 2.2.2.2 mask 3.3.3.3 route-map test
switch(config-router-af)#
```

Related Commands

Command	Description
show ip prefix-list	Displays information about IP prefix lists.

Review Draft -- Cisco Confidential

nexthop route-map

To specify that Border Gateway Protocol (BGP) routes are resolved using only the next hops that have routes that match specific characteristics, use the **nexthop route-map** command. To remove the route map, use the **no** form of this command.

nexthop route-map *name*

no nexthop route-map *name*

Syntax Description

name	Route map name. The name can be any alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Adress family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **nexthop route-map** command to configure route policy filtering for next hops.

BGP next-hop filtering allows you to specify that when a next-hop address is checked with the Routing Information Base (RIB), the underlying route for that next-hop address is passed through the route map. If the route map rejects the route, the next-hop address is treated as unreachable.

BGP marks all next hops that are rejected by the route policy as invalid and does not calculate the best path for the routes that use the invalid next-hop address.

This command requires an LAN Enterprise Services license.

Examples

This example shows how to configure a route map to filter the next-hop address:

```
switch# configure terminal
switch(config)#route-map CHECK-BGP25 deny 10
switch(config-route-map)# match ip address prefix-list FILTER25
switch(config-route-map)# match source-protocol ospf-o1
switch(config-route-map)# exit
switch(config)#ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25
switch(config)# router bgp 1.0
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# nexthop route-map CHECK-BGP25
switch(config-router-af)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
feature bgp	Enables BGP.
nexthop trigger-delay	Configures the delay timers for BGP next-hop address tracking.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

Review Draft -- Cisco Confidential

next-hop-self

To set the IP address of the router as the next hop address, use the **next-hop-self** command. To revert to the default configuration, use the **no** form of this command.

next-hop-self

no next-hop-self

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Address family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires a LAN Enterprise Services license.

Examples

This example shows how to configure the IP address of a router as the next-hop address:

```
switch# configure terminal
switch(config)# router bgp 102
switch(config-router)# neighbor 192.168.1.3 remote-as 64497
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# next-hop-self
switch(config-router-neighbor-af)#
```

Related Commands

Command	Description
address-family (BGP neighbor)	Enters the BGP neighbor address-family configuration mode.
feature bgp	Enables BGP.
show ip bgp	Displays BGP configuration information.

Review Draft -- Cisco Confidential

nexthop trigger-delay

To specify a Border Gateway Protocol (BGP) delay for triggering next-hop calculations, use the **nexthop trigger-delay** command. To set the trigger delay to the default value, use the **no** form of this command.

nexthop trigger-delay {**critical** *delay* | **non-critical** *delay*}

no nexthop trigger-delay {**critical** *delay* | **non-critical** *delay*}

Syntax Description

critical *delay*	Specifies the critical next-hop trigger delay, in milliseconds. The range is from 0 to 4294967295. The default is 3000.
non-critical *delay*	Specifies the noncritical next-hop trigger delay, in milliseconds. The range is from 0 to 4294967295. The default is 10000.

Command Default

Critical delay: 3000 milliseconds.
Noncritical delay: 10000 milliseconds.

Command Modes

Address family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **nexthop trigger-delay** command to modify when BGP processes next-hop address tracking events.

The **non-critical** *delay* value must always be set to a value that is at least equal or greater to the **critical** *delay* value.

The delay should be slightly higher than the time it takes for the Interior Gateway Protocol (IGP) to settle into a steady state after some event (IGP convergence time).

This command requires a LAN Enterprise Services license.

Examples

This example shows how to modify the next-hop address tracking delay:

```
switch# configure terminal
switch(config)# router bgp 1.0
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# nexthop trigger-delay critical 5000 non-critical 20000
```

Related Commands

Command	Description
feature bgp	Enables BGP.
nexthop route-map	Configures a route map for BGP next-hop address tracking.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

P Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with P.

Review Draft -- Cisco Confidential

password (BGP)

To configure Border Gateway Protocol (BGP) to use MD5 authentication, use the **password** command. To disable this function, use the **no** from of this command.

password [*auth-key string* | *string*]

no password [*auth-key string* | *string*]

Syntax Description

auth-key	(Optional) MD5 authentication key. You can enter an unencrypted (cleartext) key, or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The key can be from 1 to 16 characters.
string	(Optional) Neighbor password.

Command Default

None

Command Modes

BGP neighbor configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to enable an unencrypted key for a BGP neighbor:

```
switch(config)# router bgp 101
switch(config-router)# neighbor 192.0.2.1 remote-as 1.2
switch(config-route-neighbor)# password 0 myauthkey
switch(config-route-neighbor)#
```

This example shows how to disable an unencrypted authentication key for a BGP neighbor:

```
switch(config)# router bgp 101
switch(config-router)# neighbor 192.0.2.1 remote-as 1.2
switch(config-route-neighbor)# no password 0 myauthkey
switch(config-route-neighbor)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip bgp	Displays information about BGP routes.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

R Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with R.

Review Draft -- Cisco Confidential

redistribute (BGP)

To inject routes from one routing domain into the Border Gateway Protocol (BGP), use the **redistribute** command. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

redistribute {**direct** | **eigrp** *instance-tag* | **ospf** *instance-tag* | **rip** *instance-tag* | **static**} [**route-map** *map-name*]

no redistribute {{**direct** | **eigrp** *instance-tag* | **ospf** *instance-tag* | **rip** *instance-tag* | **static**} [**route-map** *map-name*]

Syntax Description

direct	Distributes routes that are directly connected on an interface.
eigrp *instance-tag*	Specifies the name of an EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
ospf *instance-tag*	Distributes routes from the OSPF protocol. This protocol is supported in the IPv4 address family. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
rip *instance-tag*	Distributes routes from the RIP protocol. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
static	Redistributes IP static routes.
route-map *map-name*	(Optional) Specifies the identifier of a configured route map. Use a route map to filter which routes are redistributed into EIGRP.

Command Default

Disabled

Command Modes

Address family configuration mode

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **redistribute** command to import routes from other routing protocols into BGP. You should always use a route map to filter these routes to ensure that BGP redistributes only the routes that you intend to redistribute.

You must configure a default metric to redistribute routes from another protocol into BGP. You can configure the default metric with the **default-metric** command or with the route map configured with the **redistribute** command.

This command requires the LAN Enterprise Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to redistribute BGP routes into an EIGRP autonomous system:

```
switch(config)# router bgp 64496
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 100
```

Related Commands

Command	Description
default-metric (BGP)	Sets the default metrics for routes redistributed into BGP.

Review Draft -- Cisco Confidential

remote-as

To specify the autonomous system (AS) number for a neighbor, use the **remote-as** command. To remove an AS number, use the **no** form of this command.

remote-as *number*

no remote-as *number*

Syntax Description

number	AS number. The format is x for a two-byte value or x.x for a four-byte value. The range is from 1 to 65535.

Command Default

None

Command Modes

Neighbor configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure the neighbor AS number:

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 10.0.0.100
switch(config-router-neighbor)# remote-as 64497
```

Related Commands

Command	Description
feature bgp	Enables BGP on the router.
neighbor	Configures BGP peers.

Review Draft -- Cisco Confidential

restart (BGP)

To restart a Border Gateway Protocol (BGP) autonomous system and remove all associated neighbors, use the **restart** command.

restart bgp *as-num*[**.***as-num*]

Syntax Description

as-num	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along; valid values are from 1 to 65535.
.*as-num*	(Optional) Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along; valid values are from 0 to 65535.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to restart the BGP autonomous system:

```
switch# restart bgp 64496
switch#
```

Related Commands

Command	Description
router bgp	Configures a BGP process.

Review Draft -- Cisco Confidential

route-map

To create a route map, enter the route-map configuration mode, or define the conditions for redistributing routes from one routing protocol into another, use the **route-map** command. To delete an entry, use the **no** form of this command.

route-map *map-tag* [**deny** | **permit**] [*sequence-number*]

no route-map *map-tag* [**permit** | **deny**] [*sequence-number*]

Syntax Description

map-tag	Route map name.
deny	(Optional) Specifies that the route or packet is not distributed if the match criteria are met for the route map.
permit	(Optional) Specifies that the route or packet is distributed if the match criteria for this route are met.
sequence-number	(Optional) Number that indicates the position a new route map has in the list of route maps already configured with the same name. The **no** form of this command deletes the position of the route map. Range: 0 to 65535.

Command Default

The **permit** keyword is the default.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If you make changes to a route map that is used by a client, you must exit the route-map configuration submode before the changes take effect in the client. The route-map changes are not propagated to its clients until you exit from the route-map configuration submode or 60 seconds expire since entering the submode.

Once you enter the route-map configuration mode, the following keywords are available:

- **continue** *sequence-number*—Continues on a different entry within the route-map. Range: 0 to 65535
- **description** *description*—Provides a description of the route map. The description can be any alphanumeric string up to 90 characters.
- **exit**—Exits from the current command mode.
- **match**—Matches the values from the specified routing table. The following keywords and arguments are available:
  - **as-path** *name* [*name*]—Specifies the autonomous system (AS) path access list to match. The name can be any alphanumeric string up to 63 characters. See the **match as-path** command for additional information.

Review Draft -- Cisco Confidential

  - **community** *name* [*name* | **exact-match**]—Specifies the BGP community list name to match. See the **match community** command for additional information.
  - **ip**—Configures the IPv4 features. The follow keywords and arguments are available:

    address {*access-list-name* [*access-list-name*] | **prefix-list** *ipv4-list-name* [*ipv4-list-name*]}—Specifies the address of the route or packet to match. See the **match ip address** command for additional information.

    multicast {**group** *address/length* | **rp** *address/length*}—Specifies the multicast attributes to match. See the **match ip multicast** command for additional information.

    next-hop—Matches the next-hop address of the route. See the **match ip next-hop** command for additional information.

    route-source—Matches the advertising source address of the route. See the **match ip route-source** command for additional information.

- **no**—Negates a command or set its defaults.
- **set**—Sets the values in the destination routing protocol. The **set** commands specify the routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets some way other than the obvious shortest path. The following keywords and arguments are available:
  - **as-path**—Prepends a string for a BGP AS-path attribute. See the **set as-path** command for additional information.
  - **comm-list**—Sets the BGP community list (for deletion). See the **set comm-list** command for additional information.
  - **community**—Sets the BGP community attribute. See the **set community** command for additional information.
  - **dampening**—Sets the BGP route flap dampening parameters. See the **set dampening** command for additional information.
  - **forwarding-address**—Sets the forwarding address. See the **set forwarding-address** command for additional information.
  - **level**—Specifies where to import the route. See the **set level** command for additional information.
  - **local-preference**—Specifies the BGP local preference path attribute. See the **set local-preference** command for additional information.
  - **metric**—Sets the metric for the destination routing protocol. See the **set metric** command for additional information.
  - **metric-type**—Sets the type of metric for the destination routing protocol. See the **set metric-type** command for additional information.
  - **origin**—Specifies the BGP origin code. See the **set origin** command for additional information.
  - **tag**—Specifies the tag value for the destination routing protocol. See the **set tag** command for additional information.
  - **weight**—Sets the BGP weight for the routing table. See the **set weight** command for additional information.

Use route maps to redistribute routes.

Review Draft -- Cisco Confidential

Redistribution

The **redistribute** router configuration command uses the *map-tag* name to reference the route map. Multiple route maps may share the same map tag name.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the **router** global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the “Examples” section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause that relates to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route map section with an explicit match specified.

Examples

This example shows how to redistribute Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes are redistributed into OSPF as external link-state advertisements (LSAs) with a metric type of Type 1, and a tag equal to 1.

```
switch(config)# router ospf 109
switch(config-route-map)# redistribute rip route-map rip-to-ospf
switch(config-route-map)# route-map rip-to-ospf permit
switch(config-route-map)# set metric 5
switch(config-route-map)# set metric-type type1
switch(config-route-map)# set tag 1
```

This example shows how to set the autonomous system path to match BGP autonomous system path access list 20:

```
switch(config)# route-map IGP2BGP
switch(config-route-map)# match as-path 20
```

This example shows how to configure that the routes matching community list 1 have the weight set to 100. Any route that has community 109 has the weight set to 100.

```
switch(config)# ip community-list 1 permit 109
switch(config)# route-map set_weight
switch(config-route-map)#  match community 1
switch(config-route-map)# set weight 100
```

This example shows how to configure that the routes matching community list 1 have the weight set to 200. Any route that has community 109 alone has the weight set to 200.

```
switch(config)# ip community-list 1 permit 109
switch(config)# route-map set_weight
switch(config-route-map)# match community 1 exact
```

Review Draft -- Cisco Confidential

```
switch(config-route-map)# set weight 200
```

This example shows how to configure that the routes match community list LIST_NAME have the weight set to 100. Any route that has community 101 alone has the weight set to 100.

```
switch(config)# ip community-list 1 permit 101
switch(config)# route-map set_weight
switch(config-route-map)# match community LIST_NAME
switch(config-route-map)# set weight 100
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

route-reflector-client (BGP)

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **route-reflector-client** command. To indicate that the neighbor is not a client, use the **no** form of this command.

route-reflector-client

no route-reflector-client

Syntax Description

This command has no arguments or keywords.

Command Default

There is no route reflector in the autonomous system.

Command Modes

BGP Neighbor address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining BGP peers will be members of the nonclient group for the local route reflector.

Examples

This example shows how to configure the local router as a route reflector to the neighbor at 192.168.0.1:

```
switch(config)# router bgp 102
switch(config-router)# neighbor 192.168.0.1 remote-as 201
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# route-reflector-client
switch(config-router-neighbor-af)#
```

Related Commands

Command	Description
address-family (BGP)	Enters the router in address family configuration mode for configuring BGP routing sessions.
neighbor	Configures a BGP neighbor.
show ip bgp	Displays entries in the BGP routing table.

Review Draft -- Cisco Confidential

router bgp

To assign an autonomous system (AS) number to a router and enter the router BGP configuration mode, use the **router bgp** command. To remove an AS number assignment, use the **no** form of this command.

router bgp *as-num*[**.***as-num*]

no router bgp *as-num*[**.***as-num*]

Syntax Description

as-num	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along; valid values are from 1 to 65535.
.*as-num*	(Optional) Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along; valid values are from 0 to 65535.

Command Default

No BGP routing process is enabled by default.

Command Modes

Address-family configuration mode
Neighbor address-family configuration mode
Router BGP configuration mode

Usage Guidelines

Release	Modification
6.0(2)N1(1)	This command was introduced.

The *as-num* is the number for the local BGP speaker and allows you to create a unique identifier for the BGP process on the router.

Once you enter the router BGP configuration mode, the following parameters are available:

- **address-family**—Configures an address-family (router, neighbor, VRF). See the **address-family (BGP)** command for information.
- **bestpath**—Changes the default best path selection algorithm. See the **bestpath** command for information.
- **cluster-id** {*cluster-id* | *cluster-ip-addr*}—Configures the Route Reflector Cluster-ID (router, VRF). Range: 1 to 4294967295. You can enter the cluster identification as a 32-bit quantity or as an IP address. To remove the cluster ID, use the **no** form of this command.
- **confederation** {**identifier** *as-num*[**.***as-num*] | **peer** *as-num*[**.***as-num*]}—Configures the AS confederation parameters as the routing domain confederation AS or the peer AS in the BGP confederation. To remove the confederation identifier, use the **no** form of this command.

  The **confederation** command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation.You can use a confederation to divide a large single autonomous system into multiple subautonomous systems and then group them into a single confederation. The subautonomous systems within the confederation exchange routing information. External peers interact with the confederation as if it were a single autonomous system.

Review Draft -- Cisco Confidential

Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

- **enforce-first-as**—Forces BGP to compare an external peer's configured AS number with the first AS in the AS-PATH of the routes received from the peer. In case of a mismatch of AS numbers, the peer is sent an error code update notification message. To disable this feature, use the **no** form of this command.
- **exit**—Exits from the current command mode.
- **fast-external-fallover**—Configures a Border Gateway Protocol (BGP) routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down. To disable BGP fast external fallover, use the **no** form of this command.

  The **fast-external-fallover** command is used to disable or enable fast external fallover for BGP peering sessions with directly connected external peers. The session is immediately reset if the link goes down. Only directly connected peering sessions are supported.

  If BGP fast external fallover is disabled, the BGP routing process waits until the default hold timer expires (three keepalives) to reset the peering session.
- **log-neighbor-changes**—Enables logging of the BGP neighbor resets. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command. The **log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

  Using the **log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host that is running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the internal buffer of the router and are not stored to the disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

  The neighbor status change messages are not tracked if the **bgp log-neighbor-changes** command is not enabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** command.

  The **eigrp log-neighbor-changes** command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the **bgp log-neighbor-changes** command.

  Use the **show logging command** to display the log for the BGP neighbor changes.
- **neighbor**—Configures a BGP neighbor (router, VRF). See the **neighbor** command for additional information.
- **no**—Negates a command or sets its defaults.
- *router-id*—Specifies the IP address to use as router-id (router, VRF).
- **template**—Enters the template command mode. See the **neighbor** command for additional information.
- **timers**—Configures the BGP-related timers (router, VRF).
  - **bestpath-limit** *interval*—Configures the timeout for the first best path after a restart, in seconds. Range: 1 to 3600. Default: 300.

Review Draft -- Cisco Confidential

  - **bgp** *interval*—Configures the different BGP keepalive and holdtimes in seconds. Range: 0 to 3600. Default: 60.
  - **prefix-peer-timeout** *interval*—Configures how long a prefix peer is maintained in seconds. Range: 0 to 1200. Default: 300:
- **vrf**—Configures the virtual router context:
  - *vrf-name*—Specifies the VRF name.
  - **management**—Specifies the configurable VRF name.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure a BGP process for autonomous system 120:

```
switch(config)# router bgp 120
switch(config-router)#
```

This example shows how to log neighbor changes for BGP in router configuration mode:

```
switch(config# bgp router 40000
switch(config-router)# log-neighbor-changes
```

This example shows how to disable the BGP fast external fallover feature. If the link through which this session is carried flaps, the connection is not reset.

```
switch(config# bgp router 64496
switch(config-router)# no fast-external-fallover
```

This example shows how all incoming updates from eBGP peers are examined to ensure that the first autonomous system number in the AS_PATH is the local AS number of the transmitting peer. The updates from the 10.100.0.1 peer are discarded if the first AS number is not 65001.

```
switch(config# router bgp 64496
switch(config-router)# bgp enforce-first-as
switch(config-router)# address-family ipv4
switch(config-router-af)# neighbor 10.100.0.1 remote-as 64496
switch(config-router-af)#
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP table.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

S Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with S.

Review Draft -- Cisco Confidential

send-community

To send the Border Gateway Protocol (BGP) community attribute to a peer, use the **send-community** command. To revert to the defaults, use the **no** form of this command.

send-community [**extended**]

no send-community [**extended**]

Syntax Description

extended	(Optional) Specifies the BGP extended community.

Command Default

No community attributes are sent to the peer.

Command Modes

BGP neighbor address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, you must configure BGP communities using the **set community** command.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure the router to send the community attribute to the neighbor 192.168.1.3:

```
switch# configure terminal
switch(config)# router bgp 102
switch(config-router)# neighbor 192.168.1.3 remote-as 64497
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)# send-community
switch(config-router-neighbor-af)#
```

Related Commands

Command	Description
set community	Defines the BGP community attributes.
show ip bgp	Displays the BGP configuration information.

Review Draft -- Cisco Confidential

set as-path

To modify an autonomous system path (as-path) for BGP routes, use the **set as-path** command. To not modify the autonomous system (AS) path, use the **no** form of this command.

set as-path {**tag** | {**prepend** *as-num*[**...***as-num*] | **last-as** *num*}}

no as-path {**tag** | {**prepend** *as-num*[*...as-num*] | **last-as** *num*}}

Syntax Description

tag	Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into Border Gateway Protocol (BGP).
prepend *as-num*	Appends the specified AS number to the autonomous system path of the route that is matched by the route map. Applies to both inbound and outbound BGP route maps. Range: 1 to 65535. You can configure more than on AS number.
last-as *num*	Prepends the last AS numbers to the as-path. Range: 1 to 10.

Command Default

Autonomous system path is not modified.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Once you enter route-map configuration mode, you can enter the **set** command.

The only global BGP metric available to influence the best path selection is the autonomous system path length. By varying the length of the autonomous system path, a BGP speaker can influence the best-path selection by a peer further away.

By allowing you to convert the tag into an autonomous system path, the **set as-path tag** variation of this command modifies the autonomous system length. The **set as-path prepend** variation allows you to prepend an arbitrary autonomous system path string to BGP routes. Usually, the local autonomous system number is prepended multiple times, increasing the autonomous system path length.

Examples

This example shows how to convert the tag of a redistributed route into an autonomous system path:

```
switch(config)# route-map test1
switch(config-route-map)# set as-path tag
```

This example shows how to prepend 100 to all the routes advertised to 10.108.1.1:

```
switch(config)# route-map test1
switch(config-route-map)# match as-path 1
switch(config-route-map)# set as-path prepend 100
```

Review Draft -- Cisco Confidential

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 10.108.1.1 remote-as 64497
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# route-map set-as-path test1 out
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

set comm-list delete

To remove communities from the community attribute of an inbound or outbound update, use the **set comm-list delete** command. To remove a previous **set comm-list delete** command, use the **no** form of this command.

set comm-list *community-list-name* **delete**

no set comm-list

Syntax Description

community-list-name	Standard or expanded community list name. The name is any alphanumeric string up to 63 characters.

Command Default

No communities are removed.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This **set** route-map configuration command removes communities from the community attribute of an inbound or outbound update using a route map to filter and determine the communities to be deleted. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each community that passes the route map **permit** clause and matches the given community list is removed from the community attribute being received from or sent to the Border Gateway Protocol (BGP) neighbor.

Each entry of a standard community list should list only one community when used with the **set comm-list delete** command. For example, in order to be able to delete communities 10:10 and 10:20, you must use the following format to create the entries:

```
switch(config)# ip community-list 500 permit 10:10
switch(config)# ip community-list 500 permit 10:20
```

The following format for a community list entry, while acceptable otherwise, does not work with the **set comm-list delete** command:

```
switch(config)# ip community-list 500 permit 10:10 10:20
```

When both the **set community** *community-number* and **set comm-list delete** commands are configured in the same sequence of a route map attribute, the deletion operation (**set comm-list delete**) is performed before the set operation (**set community** *community-number*).

Examples

This example shows how to remove communities from the community attribute of an inbound or outbound update:

Review Draft -- Cisco Confidential

```
switch(config)# route-map test1
switch(config-route-map)# match as-path 1
switch(config-route-map)# set comm-list list1 delete
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

set community

To set the Border Gateway Protocol (BGP) communities attribute, use the **set community** command. To delete the entry, use the **no** form of this command.

set community {**none** | {*aa*:*nn* [*...aa:nn*] | **additive** | **local-as** | **no-advertise** | **no-export**}}

no set community {**none** | {*aa*:*nn* | **additive** | **local-as** | **no-advertise** | **no-export**}}

Syntax Description

none	Specifies the no community attribute. You cannot configure any other keyword if you configure the **none** keyword.
aa:*nn*	Autonomous system (AS) number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered as each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space. You can configure one or more AS numbers. You can configure one or more keywords.
additive	Adds to existing community. You can configure one or more keywords.
local-as	Specifies the local-as community (well-known community). Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised to external peers or to other subautonomous systems within a confederation. You can configure one or more keywords.
no-advertise	Specifies the no-advertise community (well-known community). Routes with this community are not advertised to any peer (internal or external). You can configure one or more keywords.
no-export	Specifies the no-export community (well-known community). Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers. You can configure one or more keywords.

Command Default

No BGP communities attributes exist.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Review Draft -- Cisco Confidential

Usage Guidelines

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

Use the **route-map** global configuration command and the **match** and **set** route map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

This example shows how to configure the routes that pass the autonomous system path access list 1 to have the community set to 109:02 and 33:40. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes are not advertised to any external BGP [eBGP] peers).

```
switch(config)# route-map test1 10 permit
switch(config-route-map)# match as-path 1
switch(config-route-map)# set community 109:02 33:40
switch(config-route-map)# exit
switch(config)# route-map test1 20 permit
switch(config-route-map)# match as-path 2
switch(config-route-map)# set community no-export
```

This example shows how to configure the routes that pass the autonomous system path access list 1 to have the community set to 109:30. Routes that pass the autonomous system path access list 2 have the community set to local-as (the router does not advertise this route to peers outside the local autonomous system.

```
switch(config)# route-map test1 10 permit
switch(config-route-map)# match as-path 1
switch(config-route-map)# set community 109:30 additive
switch(config-route-map)# exit
switch(config)# route-map test1 20 permit
switch(config-route-map)# match as-path 2
switch(config-route-map)# set community local-as
```

Related Commands

Command	Description
ip community-list	Creates a community list for BGP and control access to it.
match community	Matches a BGP community.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
show ip bgp community	Displays routes that belong to specified BGP communities.

Review Draft -- Cisco Confidential

set dampening

To set the Border Gateway Protocol (BGP) route dampening factors, use the **set dampening** command. To disable this function, use the **no** form of this command.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Syntax Description

half-life	Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half life period (which is 15 minutes by default). The process of reducing the penalty occurs every 5 seconds. The range is from 1 to 45, and the default is 15.
reuse	Route that is unsuppressed if the penalty for a flapping route decreases enough to fall below this value. The process of unsuppressing routes occurs at 10-second increments. Range: 1 to 20000. Default: 750.
suppress	Route that is suppressed when its penalty exceeds this limit. The range is from 1 to 20000, and the default is 2000.
max-suppress-time	Maximum time (in minutes) that a route can be suppressed. The range is from 1 to 255, and the default is four times the *half-life* value. If the default *half-life* value is used, the maximum suppress time defaults to 60 minutes.

Command Default

Disabled

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

When a BGP peer is reset, the route is withdrawn and the flap statistics cleared. In this instance, the withdrawal does not incur a penalty even though route flap dampening is enabled.

Examples

This example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000, and the maximum suppress time to 120 minutes:

```
switch(config)# route-map test1 10 permit
```

Review Draft -- Cisco Confidential

```
switch(config-route-map)# set dampening 30 1500 10000 120
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

set etxcommunity

To set the Border Gateway Protocol (BGP) extended communities attribute, use the **set extcommunity** command. To delete the entry, use the **no** form of this command.

set extcommunity {**none** | {**generic** {**transitive** | **nontransitive**} *aa4*:*nn* [*...aa4:nn*] } | **additive**}

no set extcommunity {**none** | {**generic** {**transitive** | **nontransitive**} *aa4*:*nn* [*...aa4:nn*] } | **additive**}

Syntax Description

none	Specifies the no community attribute.
generic	Specifies the generic specific extended community type.
transitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
nontransitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
aa4:*nn*	Autonomous system number and network number. This value is configured with a 4-byte AS number and a 2-byte network number separated by a colon. The 4-byte AS number range is from 1 to 4294967295 in plaintext notation, or from 1.0 to 56636.65535 in AS.dot notation. You can enter a single community or multiple communities, each separated by a space.
additive	Adds to existing community.

Command Default

No BGP communities attributes exist.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **set extcommunity** command in a route map to set the extended community attribute in a BGP route.

You must have a match clause in a route map (even if it points to a “permit everything” list) if you want to use **set** commands.

The **set** commands specify the set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

This example shows how to configure a route map that sets the extended community to 1.5:

```
switch(config)# route-map test1 10 permit
switch(config-route-map)# match as-path 1
switch(config-route-map)# set extcommunity generic transitive 1.5
```

Review Draft -- Cisco Confidential

```
switch(config-route-map)# exit
```

Related Commands

Command	Description
ip extcommunity-list	Creates a community list for BGP and controls access to it.
match extcommunity	Matches an extended community in a route map.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
send-community	Configures BGP to propagate community attributes to BGP peers.

Review Draft -- Cisco Confidential

set extcomm-list delete

To remove extended communities from the extended community attribute of an inbound or outbound Border Gateway Protocol (BGP) update, use the **set extcomm-list delete** command. To remove a previous **set extcomm-list delete** command, use the **no** form of this command.

set extcomm-list *community-list-name* **delete**

no set extcomm-list

Syntax Description

community-list-name	Standard or expanded extended community list name. The name is any alphanumeric string up to 63 characters.

Command Default

No communities are removed.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **set extcomm-list delete** command in a route map to delete the extended community attribute in a BGP route.

You must have a match clause in a route map (even if it points to a “permit everything” list) if you want to use **set** commands.

The **set** commands specify the set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

When you configure both the **set extcommunity** *community-number* and **set ext comm-list delete** commands in the same sequence of a route map attribute, the deletion operation (**set extcomm-list delete**) is performed before the set operation (**set extcommunity** *community-number*).

Examples

This example shows how to remove extended communities from the extended community attribute of an inbound or outbound update:

```
switch# configure terminal
switch(config)# route-map test1
switch(config-route-map)# match as-path 1
switch(config-route-map)# set extcomm-list list1 delete
switch(config-route-map)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match extcommunity	Matches a BGP extended community.
set extcommunity	Sets the BGP extended communities attribute.
show route-map	Displays information about a route map.

Review Draft -- Cisco Confidential

set local-preference

To specify a preference value for the autonomous system path, use the **set local-preference** command. To delete an entry, use the **no** form of this command.

set local-preference *number-value*

no set local-preference *number-value*

Syntax Description

number-value	Preference value. Range: 0 to 4294967295. Default: 100.

Command Default

Preference value of 100 by default.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The preference is sent only to all routers in the local autonomous system.

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

You can change the default preference value with the **bgp default local-preference** command.

Examples

This example shows how to set the local preference to 100 for all routes that are included in access list 1:

```
switch# configure terminal
switch(config)# route-map test1
switch(config-router)# route-map map-preference
switch(config-route-map)# match as-path 1
switch(config-route-map)# set local-preference 100
switch(config-route-map)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show route-map	Displays information about a route map.

Review Draft -- Cisco Confidential

set metric

To set the metric value for a routing protocol, use the **set metric** command. To return to the default metric value, use the **no** form of this command.

set metric [**+** | **-**] *bandwidth-metric*

set metric *bandwidth-metric* [*delay-metric reliability-metric load-metric mtu*]

no set metric

Syntax Description

+	(Optional) Adds to the existing delay metric value.
-	(Optional) Subtracts from the existing delay metric value.
bandwidth-metric	Interior Gateway Routing Protocol (IGRP) bandwith metric, in Kb/s. The range is from 0 to 4294967295.
delay-metric	(Optional) Interior Gateway Routing Protocol (IGRP) delay metric, in 10 microsecond units. The range is from 1 to 4294967295.
reliability-metric	(Optional) IGRP reliability metric. The range is from 0 to 255.
load-metric	(Optional) IGRP load metric. The range is from 1 to 255.
mtu	(Optional) IGRP maximum transmission unit (MTU) of the path. The range is from 1 to 4294967295.

Command Default

None

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **set metric** command to modify the IGRP metric values.

Note We recommend that you consult your Cisco technical support representative before changing the default value.

When you confiture the *reliability-metric* and the *load-metric* arguments, 255 means 100 percent reliability.

Use the **+** or **-** keywords to modify the existing delay metric value. You can modify only the delay metric with these keywords.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration command to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands

Review Draft -- Cisco Confidential

specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

This example shows how to set the bandwith metric value for the routing protocol to 100:

```
switch# configure terminal
switch(config)# route-map set-metric
switch(config-route-map)# set metric 100
switch(config-route-map)#
```

This example shows how to increase the bandwith metric value for the routing protocol by 100:

```
switch# configure terminal
switch(config)# route-map set-metric
switch(config-route-map)# set metric +100
switch(config-route-map)#
```

Related Commands

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show route-map	Displays information about a route map.

Review Draft -- Cisco Confidential

set metric-type

To set the metric type for the destination routing protocol, use the **set metric-type** command. To return to the default, use the **no** form of this command.

set metric-type {**internal** | **type-1** | **type-2**}

no set metric-type {**internal** | **type-1** | **type-2**}

Syntax Description

internal	Specifies the Interior Gateway Protocol (IGP) metric as the multi-exit discriminator (MED) for BGP.
type-1	Specifies the Open Shortest Path First (OSPF) external Type 1 metric.
type-2	Specifies the OSPF external Type 2 metric.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Note This command is not supported for redistributing routes into Border Gateway Protocol (BGP).

Examples

This example shows how to set the metric type of the destination protocol to OSPF external Type 1:

```
switch# configure terminal
switch(config)# route-map map-type
switch(config-route-map)# set metric-type type-1
switch(config-route-map)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show ip community-list	Displays information about a community list.
show ip extcommunity-list	Displays information about an extended community list.
show ip prefix-list	Displays information about IPv4 prefix lists.
show route-map	Displays information about a route map.

Review Draft -- Cisco Confidential

set origin

To set the Border Gateway Protocol (BGP) origin code, use the **set origin** command. To delete the entry, use the **no** form of this command.

set origin {**egp** *as-num* [:*as-num*] | **igp** | **incomplete**}

no set origin

Syntax Description

egp *as-num*	Specifies the autonomous system (AS) number for a remote exterior gateway protocol (EGP) system. You can specify the AS number as a 2-byte integer or a 4-byte integer in aa:nn format. Range is from 1 to 65535.
igp	Specifies a local interior gateway protocol (IGP) system.
incomplete	Specifies an unknown heritage.

Command Default

Default origin, based on route in main IP routing table.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set route-map** configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

This example shows how to set the origin of routes that pass the route map to IGP:

```
switch# configure terminal
switch(config)# route-map set_origin
switch(config-route-map)# match as-path 10
switch(config-route-map)# set origin igp
switch(config-route-map)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show ip community-list	Displays information about a community list.
show ip extcommunity-list	Displays information about an extended community list.
show ip prefix-list	Displays information about IPv4 prefix lists.
show route-map	Displays information about a route map.

Review Draft -- Cisco Confidential

set tag

To set a tag value of the destination routing protocol, use the **set tag** command. To delete the entry, use the **no** form of this command.

set tag *tag-value*

no set tag *tag-value*

Syntax Description

tag-value	Name for the tag. The value is an integer from 0 to 4294967295.

Command Default

If not specified, the default action is to *forward* the tag in the source routing protocol onto the new destination protocol.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

This example shows how to set the tag value of the destination routing protocol to 5:

```
switch(config)# route-map test
switch(config-route-map)# set tag 5
```

Related Commands

Command	Description
match tag	Redistributes routes in the routing table that match the specified tags.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

Review Draft -- Cisco Confidential

set weight

To specify the Border Gateway Protocol (BGP) weight for the routing table, use the **set weight** command. To delete an entry, use the **no** form of this command.

set weight *number*

no set weight [*number*]

Syntax Description

number	Weight value. Range: 0 to 65535.

Command Default

The weight is not changed by the specified route map.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global **neighbor** commands.

Examples

This example shows how to set the BGP weight for the routes that match the autonomous system path access list to 200:

```
switch# configure terminal
switch(config)# route-map set-weight
switch(config-route-map)# match as-path 10
switch(config-route-map)# set weight 200
switch(config-route-map)#
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show ip community-list	Displays information about a community list.
show ip extcommunity-list	Displays information about an extended community list.
show ip prefix-list	Displays information about IPv4 prefix lists.
show route-map	Displays information about a route map.

Review Draft -- Cisco Confidential

shutdown (BGP)

To shut down an instance of the Border Gateway Protocol (BGP), use the **shutdown** command. To disable this function, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **shutdown** command to disable an instance of BGP without removing the configuration.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to disable BGP 64496:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# shutdown
switch(config-router)#
```

Related Commands

Command	Description
show bgp	Displays BGP routes.

Review Draft -- Cisco Confidential

soft-reconfiguration inbound (BGP)

To configure the switch software to start storing Border Gateway Protocol (BGP) peer updates, use the **soft-reconfiguration** command. To not store received updates, use the no form of this command.

soft-reconfiguration inbound

no soft-reconfiguration inbound

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Neighbor address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability.

Examples

This example shows how to configure the soft reconfiguration on the neighbor at 192.168.0.1:

```
switch# configure terminal
switch(config)# router bgp 102
switch(config-router)# neighbor 192.168.0.1 remote-as 201
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# soft-reconfiguration inbound
switch(config-router-neighbor-af)#
```

Related Commands

Command	Description
address-family (BGP)	Enters the router in address family configuration mode for configuring BGP routing sessions.
neighbor	Configures a BGP neighbor.
show ip bgp neighbors	Displays BGP peer information.

Review Draft -- Cisco Confidential

suppress-inactive

To advertise the active routes to a Border Gateway Protocol (BGP) peer only, use the **suppress-inactive** command. To remove the restriction, use the **no** form of this command. To return to the default setting, use the **default** form of this command.

suppress-inactive

no default suppress-inactive

Syntax Description

This command has no arguments or keywords.

Command Default

BGP advertises routes to a peer as soon as they are installed in the local routing table, even if the routes are not the active routes in the table.

Command Modes

Neighbor address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **suppress-inactive** command to advertise only active routes to a BGP peer.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to create a summary address. The path advertised for this route is an autonomous system set consisting of all elements contained in all paths that are being summarized.

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1/8 remote-as 64497
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor af)# suppress-inactive
switch(config-router-neighbor af)#
```

Related Commands

Command	Description
route-map	Creates a route map.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) **show** commands.

Review Draft -- Cisco Confidential

show bgp

To display Border Gateway Protocol (BGP) routes, use the **show bgp** command.

show bgp {**all** | **ipv4** {**unicast** | **multicast**} [*addr* | *prefix* [**longer-prefixes**]] [**vrf** *vrf-name* | **all**]}

Syntax Description

all	Displays BGP information for all address families.
ipv4	Displays BGP information for the IPv4 address family.
unicast	Displays BGP information for the unicast address family.
multicast	Displays BGP information for the multicast address family.
addr	(Optional) Network from the selected address family. The format is A.B.C.D for IPv4.
prefix	(Optional) Prefix from the selected address family. The format is A.B.C.D/length for IPv4.
longer-prefixes	(Optional) Displays the prefix and any more specific routes.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show bgp** command to display information about BGP.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display an entry in the BGP table:

```
switch# show bgp ipv4 multicast
BGP routing table information for VRF default, address family IPv4 Multicast
BGP table version is 5, local router ID is 2.2.2.3
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath

   Network            Next Hop            Metric     LocPrf     Weight Path
  192.168.1.3         0.0.0.0                             100      32768 i
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear bgp	Clears entries in the BGP table.

Review Draft -- Cisco Confidential

show bgp community

To display Border Gateway Protocol (BGP) routes that match a community, use the **show bgp community** command.

show bgp {{**ip** | **ipv4**} {**unicast** | **multicast**}} **community** [*as-number*] [**no-advertise**] [**no-export**] [**no-export-subconfed**] [**exact-match**]} [**vrf** *vrf-name*]

Syntax Description

ip	Displays BGP information for the IPv4 address family.
ipv4	Displays BGP information for the IPv4 address family.
unicast	Displays BGP information for the unicast address family.
multicast	Displays BGP information for the multicast address family.
as-number	(Optional) AS number. The AS number can be a 16-bit integer or a 32-bit integer in the form of <higher 16-bit decimal number>.<lower 16-bit decimal number>.
no-advertise	(Optional) Displays the no-advertise community.
no-export	(Optional) Displays the no-export community.
no-export-subconfed	(Optional) Displays the no-export-subconfed community.
exact-match	(Optional) Displays an exact match of the community.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Command History

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the routes that match a community:

```
switch# show bgp ip multicast community no-advertise
```

Related Commands

Command	Description
ip community-list	Creates a community list.

Review Draft -- Cisco Confidential

show bgp community-list

To display Border Gateway Protocol (BGP) routes that match a community list, use the **show bgp community-list** command.

show bgp {{**ip** | **ipv4**} {**unicast** | **multicast**}} **community-list** *commlist-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description

ip	Displays BGP information for the IPv4 address family.
ipv4	Displays BGP information for the IPv4 address family.
unicast	Displays BGP information for the unicast address family.
multicast	Displays BGP information for the multicast address family.
commlist-name	Name of a community-list. The commlist-name can be any case-sensitive, alphanumeric string up to 63 characters.
exact-match	(Optional) Displays an exact match of the communities.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the routes that match a community list:

```
switch(config)# show bgp ip unicast community-list test1
```

Related Commands

Command	Description
ip community-list	Creates a community list.

Review Draft -- Cisco Confidential

show bgp extcommunity

To display Border Gateway Protocol (BGP) routes that match an extended community, use the **show bgp extcommunity** command.

show bgp {{**ip** | **ipv4**} {**unicast** | **multicast**}} **extcommunity 4byteas-generic** {**non-transitive** | **transitive**} [*as4-number*] [**exact-match**] [**vrf** *vrf-name*]

Syntax Description

ip	Displays BGP information for the IPv4 address family.
ipv4	Displays BGP information for the IPv4 address family.
unicast	Displays BGP information for the unicast address family.
multicast	Displays BGP information for the multicast address family.
4byteas-generic	Displays the routes that match the generic specifice extended communities.
non-transitive	Displays the routes that match the nontransitive extended communities.
transitive	Displays the routes that match the transitive extended communities.
as4-number	AS number. The *as4-number* is a 32-bit integer in the form of a plaintext integer or <higher 16-bit decimal number>.<lower 16-bit decimal number> .
exact-match	(Optional) Displays an exact match of the extended community.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) context name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the routes that match an extended community:

```
switch(config)# show bgp ip unicast extcommunity 4byteas-generic transitive 1.3:30
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list.

Review Draft -- Cisco Confidential

show bgp extcommunity-list

To display Border Gateway Protocol (BGP) routes that match an extended community list, use the **show bgp extcommunity-list** command.

show bgp {{**ip** | **ipv4**} {**unicast** | **multicast**}} **extcommunity-list** *commlist-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description

ip	Displays BGP information for the IPv4 address family.
ipv4	Displays BGP information for the IPv4 address family.
unicast	Displays BGP information for the unicast address family.
multicast	Displays BGP information for the multicast address family.
commlist-name	Name of an extended community-list. The *commlist-name* can be any case-sensitive, alphanumeric string up to 63 characters.
exact-match	(Optional) Displays an exact match of the extended communities.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the routes that match a community list:

```
switch(config)# show bgp ipv4 unicast extcommunity-list test1
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list.

Review Draft -- Cisco Confidential

show bgp neighbors

To display Border Gateway Protocol (BGP) neighbors, use the **show bgp neighbors** command.

show bgp {**ip** | **ipv4**} {**unicast** | **multicast**} **neighbors** [*addr* [**advertised-routes** | **flap-statistics** | **paths** | **received-routes** | **routes** [**advertised** | **dampened** | **received**]]] [**vrf** {**all** | *vrf-name*}]

Syntax Description

ip	Displays the IPv4 neighbor information.
ipv4	Displays the IPv4 neighbor information.
unicast	Displays the unicast neighbor information.
multicast	Displays the multicast neighbor information.
addr	IPv4 address. The format is x.x.x.x
advertised-routes	(Optional) Displays all the routes advertised to this neighbor.
flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.
paths	(Optional) Displays AS paths learned from this neighbor.
received-routes	(Optional) Displays all the routes received from this neighbor.
routes	(Optional) Displays the routes received or advertised to or from this neighbor.
advertised	(Optional) Displays all the routes advertised for this neighbor.
dampened	(Optional) Displays all dampened routes received from this neighbor.
received	(Optional) Displays all the routes received from this neighbor.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	Specifies all VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP neighbors:

```
switch(config)# show bgp ip unicast neighbors
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip bgp neighbors	Displays the IPv4 BGP information.

Review Draft -- Cisco Confidential

show bgp sessions

To display Border Gateway Protocol (BGP) sessions, use the **show bgp sessions** command.

show bgp sessions [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP sessions:

```
switch# show bgp sessions
Total peers 2, established peers 0
ASN 102
VRF default, local ASN 102
peers 2, established peers 0, local router-id 2.2.2.3
State: I-Idle, A-Active, O-Open, E-Established, C-Closing, S-Shutdown

Neighbor        ASN    Flaps LastUpDn|LastRead|LastWrit St Port(L/R)  Notif(S/R)
10.0.0.100      64497 0     01:31:58|never   |never    I  0/0        0/0
192.168.1.3         0 0     00:03:25|never   |never    I  0/0        0/0
switch#
```

Related Commands

Command	Description
clear bgp	Clears BGP sessions.

Review Draft -- Cisco Confidential

show bgp statistics

To display Border Gateway Protocol (BGP) traffic statistics, use the **show bgp statistics** command.

show bgp statistics

Syntax Description

This command has no argument or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP traffic statistics:

```
switch# show bgp statistics

Neighbor aggregated statistics (sent/received)
 Msgs                 Bytes                Opens                Updates

 0/0                  0/0                  0/0                  0/0


 Keepalives           Notifications        Route-refresh        Capabilities

 0/0                  0/0                  0/0                  0/0


BGP I/O Information
Active Open attempts               : 0
Passive Open attempts              : 0
BGP I/O Open loops                 : 117
BGP I/O Open calls                 : 0
BGP I/O Open recv calls            : 0
BGP I/O Send calls                 : 0
BGP I/O Recv calls                 : 0
BGP I/O Write calls                : 0
BGP I/O Write loops                : 1
BGP I/O Write loop yields          : 0
BGP I/O Read calls                 : 0
BGP I/O Read loops                 : 117
BGP I/O Read loop yields           : 0
BGP I/O process nlri yields        : 0
BGP I/O process withdraw yields    : 0
BGP Read time exceeded             : 0
```

Review Draft -- Cisco Confidential

```
BGP Update send pending             : 0
BGP Update buffer not available     : 0
BGP Update walk suspended           : 0
BGP Yielded in updates              : 0
BGP Yielded in packing              : 0
BGP No sendbuf for peer             : 0
BGP No withdraw buf for peer        : 0
BGP Yields in update peer loop      : 0
No updates pending or no buffers    : 1
No data to write                    : 1
Msg queue recv errors               : 0
Sockets create/accept/close         : 2/0/0
Sockets create retries/failures     : 0/0
switch#
```

Related Commands

Command	Description
clear bgp	Clears BGP sessions.

Review Draft -- Cisco Confidential

show ip bgp

To display entries in the Border Gateway Protocol (BGP) table, use the **show ip bgp** command.

show ip bgp [*ip-addr* | *ip-prefix* [**longer-prefixes**]] [**received-paths**] [**regexp** *expression*] [**route-map** *map-name*] [**summary**] [**vrf** *vrf-name*]

Syntax Description

ip-addr	(Optional) Network from the BGP route table. The format is x.x.x.x.
ip-prefix	(Optional) Prefix from the BGP route table. The format is x.x.x.x/length.
longer-prefixes	(Optional) Displays the prefix and any more specific routes.
received-paths	(Optional) Displays paths stored for soft reconfiguration.
regexp *expression*	(Optional) Displays information that matches the regular expression.
route-map *map-name*	(Optional) Displays routes that match the route map. The map name can be any case-sensitive, alphanumeric string up to 63 characters.
summary	(Optional) Displays the summary of the routes.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP route table:

```
switch(config-router)# show ip bgp
```

Related Commands

Command	Description
clear ip bgp	Clears entries in the BGP route table.

Review Draft -- Cisco Confidential

show ip bgp all

To display the Border Gateway Protocol (BGP) entries for all address families, use the **show ip bgp all** command.

show ip bgp all [*ip-addr* | *ip-prefix* [**longer-prefixes**]] [**filter-list** *list-name*] [**community-list** *commlist-name* [**exact-match**]] [**flap-statistics**] [**nexthop-database**] [**received-paths**] [**regexp** *expression*][**route-map** *map-name*] [**summary**] [**vrf** {*vrf-name* | **all**}]

show ip bgp all community [*comm-name*] [{{**internet** | **no-advertise** | **no-export** | **no-export-subconfed**} | **exact-match**}] [**vrf** {*vrf-name* | **all**}]

show ip bgp all extcommunity 4byteas-generic {**non-transitive** | **transitive**} [*as4-number*] [**exact-match**] [**vrf** {*vrf-name* | **all**}]

show ip bgp all dampening {**dampened-paths** [**regexp** *expression*] | **flap-statistics** | **history-paths** [**regexp** *expression*] | **parameters**} [**vrf** {*vrf-name* | **all**}]

show ip bgp all neighbors [*ip-addr* [**advertised-routes** | **flap-statistics** | **paths** | **received-routes** | **routes** [**advertised** | **dampened** | **received**]]] [**vrf** {*vrf-name* | **all**}]

Syntax Description

ip-addr	(Optional) Network from the BGP route table. The format is x.x.x.x.
ip-prefix	(Optional) Prefix from the BGP route table. The format is x.x.x.x/length.
longer-prefixes	(Optional) Displays the prefix and any more specific routes.
filter-list	(Optional) Displays BGP routes that match a filter list.
list-name	Name of a filter list. The name can be any case-sensitive, alphanumeric string up to 63 characters.
community-list *commlist-name*	(Optional) Display routes matching the community-list. The *commlist-name* can be any case-sensitive, alphanumeric string up to 63 characters.
exact-match	(Optional) Displays an exact match of the communities.
flap-statistics	Displays flap statistics for routes.
nexthop-database	(Optional) Displays the BGP next-hop database.
received-paths	(Optional) Displays paths stored for soft reconfiguration.
regexp *expression*	(Optional) Displays information that matches the regular expression.
route-map *map-name*	(Optional) Displays routes that match the route map. The map name can be any case-sensitive, alphanumeric string up to 63 characters.
summary	(Optional) Displays the summary of the routes.
community	Displays BGP routes that match a community list.
community-number	(Optional) Community number. Valid value is a community number in the range from 1 to 4294967200, or **AA**:**NN** (autonomous system-community number/2-byte number).
no-export	(Optional) Displays routes with this community that are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation.
no-advertise	(Optional) Displays routes that are not advertise to any peer (internal or external).

Review Draft -- Cisco Confidential

no-export-subconfed	(Optional) Displays routes that are part of the well-known community no-export-subconfed.
internet	(Optional) Displays routes that are part of the well-known community internet community.
extcommunity	Displays routes that match an extended community.
4byteas-generic	(Optional) Displays the routes that match the generic specifice extended communities.
non-transitive	(Optional) Displays the routes that match the non-transitive extended communities.
transitive	(Optional) Displays the routes that match the transitive extended communities.
as4-number	(Optional) AS number. The *as4-number* is a 32-bit integer in the form of a plaintext integer or <higher 16-bit decimal number>.<lower 16-bit decimal number> .
exact-match	(Optional) Displays an exact match of the extended community.
dampening	Displays all dampening information.
dampened-paths	(Optional) Displays all dampened paths.
regexp *expression*	(Optional) Display information that matches the regular expression.
history-paths	(Optional) Displays all history paths.
parameters	(Optional) Displays all dampening parameters.
neighbors	Displays all BGP neigbors.
advertised-routes	(Optional) Displays all the routes advertised to this neighbor.
flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.
paths	(Optional) Displays AS paths learned from this neighbor.
received-routes	(Optional) Displays all the routes received from this neighbor.
routes	(Optional) Displays the routes received or advertised to or from this neighbor.
advertised	(Optional) Displays all the routes advertised for this neighbor.
dampened	(Optional) Displays all dampened routes received from this neighbor.
received	(Optional) Displays all the routes received from this neighbor.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies the VFR reserved all name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Review Draft -- Cisco Confidential

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP entries for all address families:

```
switch# show ip bgp all
BGP routing table information for VRF default, address family IPv4 Multicast
BGP table version is 5, local router ID is 2.2.2.3
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath

   Network            Next Hop            Metric     LocPrf     Weight Path
  192.168.1.3/2          0.0.0.0                            100      32768 i
switch#
```

This example shows how to display a summary of the state of the BGP route table:

```
switch# show ip bgp all summary
BGP summary information for VRF default, address family IPv4 Multicast
BGP router identifier 2.2.2.3, local AS number 102
BGP table version is 5, IPv4 Multicast config peers 2, capable peers 0
1 network entries and 1 paths using 104 bytes of memory
BGP attribute entries [1/124], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.100      4 64497       0       0        0    0    0 03:20:10 Idle
192.168.1.3     4     0       0       0        0    0    0 01:51:38 Idle
switch#
```

Related Commands

Command	Description
clear ip bgp	Clears entries in the BGP route table.

Review Draft -- Cisco Confidential

show ip bgp community

To display Border Gateway Protocol (BGP) routes that match a community list, use the **show ip bgp community** command.

show ip bgp community {*community-number*] [{**internet** | **no-advertise** | **no-export** | **no-export-subconfed**}} [**vrf** {*vrf-name* | **all**}]

Syntax Description

community-number	Community number. Valid value is a community number in the range from 1 to 4294967200, or **AA**:**NN** (autonomous system-community number/2-byte number).
internet	Displays routes that are part of the well-known community internet community.
no-advertise	Displays routes that are not advertise to any peer (internal or external).
no-export	Displays routes with this community that are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation.
no-export-subconfed	Displays routes that are part of the well-known community no-export-subconfed.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies the reserved all VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the routes that are part of the 201 BGP community:

```
switch# show ip bgp community 201
```

This example shows how to display the routes that are part of the no-advertise BGP community and all VRF:

```
switch# show ip bgp community no-advertise
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
set community	Sets the attributes for BGP communities.
show ip bgp community-list	Displays BGP routes that are permitted by the BGP community list.
show ip bgp community exact-match	Displays the routes that have exactly the same specified BGP communities.

Review Draft -- Cisco Confidential

show ip bgp community exact-match

To display routes that matches a specific Border Gateway Protocol (BGP) community, use the **show ip bgp community exact-match** command.

show ip bgp community *community-number* **exact-match** [**vrf** {**all** | *vrf-name*}]

Syntax Description

community-number	Community number. Valid value is a community number in the range from 1 to 4294967200, or **AA**:**NN** (autonomous system-community number/2-byte number).
exact-match	Displays only routes that have exactly the same specified communities.
all	(Optional) Specifies the reserved all VRF.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the routes that have exactly the same specified BGP communities:

```
switch# show ip bgp community 201 exact-match
```

Related Commands

Command	Description
set community	Sets the attributes for BGP communities.
show ip bgp community	Displays the BGP routes that match a community list.
show ip bgp community-list	Displays BGP routes that are permitted by the BGP community list.

Review Draft -- Cisco Confidential

show ip bgp community-list

To display Border Gateway Protocol (BGP) routes that are permitted by the BGP community list, use the **show ip bgp community-list** command.

show ip bgp [**ipv4** {**unicast** | **multicast**} | **all**] **community-list** *commlist-name* [**exact-match**]} [**vrf** *vrf-name*]

Syntax Description

ipv4	(Optional) Displays BGP information for the IPv4 address family.
unicast	Displays BGP information for the unicast address family.
multicast	Displays BGP information for the multicast address family.
all	Displays BGP information for all address families.
community-list *commlist-name*	Display routes matching the community-list. The *commlist-name* can be any case-sensitive, alphanumeric string up to 63 characters.
exact-match	(Optional) Displays an exact match of the communities.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display routes that match a community list:

```
switch(config)# show ip bgp community-list test1
```

Related Commands

Command	Description
ip community-list	Creates a community list.

Review Draft -- Cisco Confidential

show ip bgp dampening

To display Border Gateway Protocol (BGP) dampening information, use the **show ip bgp dampening** command.

show ip bgp [**ipv4** {**unicast** | **multicast**} | **all**] **dampening** {**dampened-paths** [**regexp** *expression*] | **flap-statistics** | **history-paths** [**regexp** *expression*] | **parameters**} [**vrf** *vrf-name*]

Syntax Description

ipv4	(Optional) Displays BGP information for the IPv4 address family.
unicast	Displays BGP information for the unicast address family.
multicast	Displays BGP information for the multicast address family.
all	(Optional) Displays BGP information for all address families.
dampened-paths	Displays all dampened paths.
regexp *expression*	(Optional) Display information that matches the regular expression.
flap-statistics	Displays flap statistics for routes.
history-paths	Displays all history paths.
parameters	Displays all dampening parameters.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the dampening information:

```
switch(config)# show ip bgp dampening dampened-paths
```

Related Commands

Command	Description
address-family (BGP router)	Configures BGP parameters.
dampening (BGP)	Configures the route flap dampening.

Review Draft -- Cisco Confidential

show ip bgp extcommunity

To display Border Gateway Protocol (BGP) routes that match an extended community, use the **show ip bgp extcommunity** command.

show ip bgp extcommunity generic {**non-transitive** | **transitive**} [*as4-number*] [**exact-match**] [**vrf** *vrf-name*]

Syntax Description

generic	Displays the routes that match the generic specifice extended communities.
non-transitive	Displays the routes that match the non-transitive extended communities.
transitive	Displays the routes that match the transitive extended communities.
as4-number	(Optional) AS number. The *as4-number* is a 32-bit integer in the form of a plaintext integer or <higher 16-bit decimal number>.<lower 16-bit decimal number> .
exact-match	(Optional) Displays an exact match of the extended community.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display routes that match an extended community:

```
switch(config)# show ip bgp extcommunity generic transitive 1.3:30
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list.

Review Draft -- Cisco Confidential

show ip bgp extcommunity-list

To display Border Gateway Protocol (BGP) routes that match an extended community list, use the **show ip bgp extcommunity-list** command.

show ip bgp extcommunity-list *commlist-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description

commlist-name	Name of an extended community-list. The *commlist-name* can be any case-sensitive, alphanumeric string up to 63 characters.
exact-match	(Optional) Displays an exact match of the extended communities.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display routes that match a community list:

```
switch(config)# show ip bgp extcommunity-list test1
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list.

Review Draft -- Cisco Confidential

show ip bgp filter-list

To display Border Gateway Protocol (BGP) routes that match a filter list, use the **show ip bgp filter-list** command.

show ip bgp filter-list *list-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description

list-name	Name of a filterlist. The name can be any case-sensitive, alphanumeric string up to 63 characters.
exact-match	(Optional) Displays an exact match of the filter.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display routes that match a filter list:

```
switch(config)# show ip bgp filter-list test1
```

Related Commands

Command	Description
filter-list	Assigns an autonomous system (AS) path filter to a BGP peer.
show ip bgp all	Displays the BGP entries for all address families.

Review Draft -- Cisco Confidential

show ip bgp flap-statistics

To display Border Gateway Protocol (BGP) flap statistics, use the **show ip bgp flap-statistics** command.

show ip bgp flap-statistics [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the flap statistics:

```
switch(config)# show ip bgp flap-statistics
```

Related Commands

Command	Description
clear bgp flap-statistics	Clears BGP route flap statistics.

Review Draft -- Cisco Confidential

show ip bgp neighbors

To display Border Gateway Protocol (BGP) neighbors, use the **show ip bgp neighbors** command.

show ip bgp neighbors [*addr* [**advertised-routes | flap-statistics | paths | received-routes | routes** [**advertised | dampened | received**]]] [**vrf** {**all** | *vrf-name*}]

Syntax Description

addr	(Optional) IPv4 address. The format is x.x.x.x
advertised-routes	(Optional) Displays all the routes advertised to this neighbor.
flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.
paths	(Optional) Displays AS paths learned from this neighbor.
received-routes	(Optional) Displays all the routes received from this neighbor.
routes	(Optional) Displays the routes received or advertised to or from this neighbor.
advertised	(Optional) Displays all the routes advertised for this neighbor.
dampened	(Optional) Displays all dampened routes received from this neighbor.
received	(Optional) Displays all the routes received from this neighbor.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP neighbors:

```
switch(config)# show ip bgp neighbors
```

Related Commands

Command	Description
neighbor	Configures BGP neighbors.

Review Draft -- Cisco Confidential

show ip bgp nexthop

To display Border Gateway Protocol (BGP) next-hop information, use the **show ip bgp nexthop** command.

show ip bgp nexthop *addr* [**vrf** *vrf-name*]

Syntax Description

addr	IPv4 address. The format is x.x.x.x
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP next-hop information:

```
switch(config)# show ip bgp nexthop 192.0.2.1
```

Related Commands

Command	Description
show ip bgp neighbors	Displays BGP neighbor information.

Review Draft -- Cisco Confidential

show ip bgp nexthop-database

To display Border Gateway Protocol (BGP) next-hop database, use the **show ip bgp nexthop-database** command.

show ip bgp nexthop-database [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP next-hop database:

```
switch(config)# show ip bgp nexthop-database
```

Related Commands

Command	Description
show ip bgp neighbors	Displays BGP neighbor information.

Review Draft -- Cisco Confidential

show ip bgp paths

To display all the Border Gateway Protocol (BGP) paths in the database, use the **show ip bgp paths** command.

show ip bgp paths

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP paths in the database:

```
switch(config)# show ip bgp paths
Address    Hash Refcount     Metric Path
0x5a5e46bc 2001        1          0 i
switch#
```

Related Commands

Command	Description
maximum-paths	Controls the maximum number of parallel routes that the Border Gateway Protocol (BGP) can support.
show ip bgp	Displays the BGP table information.
show ip bgp neighbors	Displays BGP neighbor information.

Review Draft -- Cisco Confidential

show ip bgp peer-policy

To display Border Gateway Protocol (BGP) peer policy template information, use the **show ip bgp peer-policy** command.

show ip bgp peer-policy *name*

Syntax Description

name	Name of a BGP template. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Command History

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP peer policy:

```
switch(config)# show ip bgp peer-policy test1
```

Related Commands

Command	Description
inherit peer-policy	Inherits a peer policy template for a neighbor.
template peer-policy	Configures a peer policy template.

Review Draft -- Cisco Confidential

show ip bgp peer-session

To display Border Gateway Protocol (BGP) peer session template information, use the **show ip bgp peer-session** command.

show ip bgp peer-session *name*

Syntax Description

name	Name of a BGP template. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP peer session:

```
switch(config)# show ip bgp peer-session test1
```

Related Commands

Command	Description
inherit peer-session	Inherits a peer session template for a neighbor.
template peer-session	Configures a peer session template.

Review Draft -- Cisco Confidential

show ip bgp peer-template

To display Border Gateway Protocol (BGP) peer template information, use the **show ip bgp peer-template** command.

show ip bgp peer-template *name*

Syntax Description

name	Name of a BGP template. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP peer template:

```
switch(config)# show ip bgp peer-template peer1
```

Related Commands

Command	Description
inherit peer-template	Inherits a peer template for a neighbor.
template peer	Configures a peer template.

Review Draft -- Cisco Confidential

show ip bgp prefix-list

To display Border Gateway Protocol (BGP) routes that match a prefix list, use the **show ip bgp prefix-list** command.

show ip bgp prefix-list *list-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description

list-name	Name of a prefix list. The commlist-name can be any case-sensitive, alphanumeric string up to 63 characters.
exact-match	(Optional) Displays an exact match of the filter.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display routes that match a prefix list:

```
switch(config)# show ip bgp prefix-list test1
```

Related Commands

Command	Description
maximum-prefix	Controls the number of prefixes that can be received from a BGP neighbor.

Review Draft -- Cisco Confidential

show ip bgp received-paths

To display the routes received from a Border Gateway Protocol (BGP) peer, use the **show ip bgp received-paths** command.

show ip bgp received-paths [**vrf** *vrf-name* | **all**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the received routes from a BGP peer:

```
switch(config)# show ip bgp received-paths
```

Related Commands

Command	Description
show ip bgp neighbors	Displays BGP neighbor information.

Review Draft -- Cisco Confidential

show ip bgp route-map

To display the Border Gateway Protocol (BGP) route maps from the BGP table, use the **show ip bgp route-map** command.

show ip bgp route-map *route-map-name* [**vrf** *vrf-name* | **all**]

Syntax Description

route-map-name	Route map name.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the BGP route maps from the BGP table:

```
switch(config)# show ip bgp route-map
```

Related Commands

Command	Description
route-map	Creates route maps.
clear ip bgp	Clear BGP routes from the BGP table.

Review Draft -- Cisco Confidential

show ip bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the **show ip bgp summary** command.

show ip bgp summary [**vrf** *vrf-name* | **all**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise Services license.

Examples

This example shows how to display the status of BGP connections:

```
switch(config)# show ip bgp summary
```

Related Commands

Command	Description
maximum-prefix	Controls the number of prefixes that can be received from a BGP neighbor.
router bgp	Assigns an autonomous system (AS) number to a router.

Review Draft -- Cisco Confidential

show ip community-list

To display community lists for the Border Gateway Protocol (BGP), use the **show ip community-list** command.

show ip community-list [*name*]

Syntax Description

name	(Optional) Name of the community list. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Review Draft -- Cisco Confidential

show ip prefix-list

To display prefix lists for the Border Gateway Protocol (BGP), use the **show ip prefix-list** command.

show ip prefix-list [*name*]

Syntax Description

name	(Optional) Name of community list. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the prefix lists:

```
switch(config)# show ip prefix-list
```

Related Commands

Command	Description
ip prefix-list	Configures a BGP prefix list.

Review Draft -- Cisco Confidential

show mac-list

To display the entries in a MAC list, use the **show mac-list** command.

show mac-list [*name*]

Syntax Description

name	(Optional) MAC list name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

No match values are defined.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Enterprise license.

Examples

This example shows how to display information about the Red MAC list:

```
switch(config)# show mac-list Red
```

Related Commands

Command	Description
mac-list	Creates a MAC list.
match mac-list	Matches a MAC address in a MAC list.

Review Draft -- Cisco Confidential

show vrf

To display the virtual routing and forwarding (VRF) instances, use the **show vrf** command.

show vrf

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the VRF instances configured on the switch:

```
switch# show vrf
VRF-Name                           VRF-ID State   Reason
default                                 1 Up      --
management                              2 Up      --
switch#
```

Related Commands

Command	Description
vrf	Configures a VRF instance.
vrf context	Creates a VRF instance.
vrf member	Adds an interface to a VRF.

Review Draft -- Cisco Confidential

show vrf detail

To display the detailed information of virtual routing and forwarding (VRF) instances, use the **show vrf detail** command.

show vrf detail

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

By default, this command displays the detailed information of the default VRF and management VRF.

This command does not require a license.

Examples

This example shows how to display the detailed information of VRF instances configured on the switch:

```
switch# show vrf detail
VRF-Name: default, VRF-ID: 1, State: Up
    Table-ID: 0x80000001, AF: IPv6, Fwd-ID: 0x80000001, State: Up
    Table-ID: 0x00000001, AF: IPv4, Fwd-ID: 0x00000001, State: Up

VRF-Name: management, VRF-ID: 2, State: Up
    Table-ID: 0x80000002, AF: IPv6, Fwd-ID: 0x80000002, State: Up
    Table-ID: 0x00000002, AF: IPv4, Fwd-ID: 0x00000002, State: Up

switch#
```

Related Commands

Command	Description
vrf	Configures a VRF instance.
vrf context	Creates a VRF instance.
vrf member	Adds an interface to a VRF.

Review Draft -- Cisco Confidential

show vrf interface

To display the virtual routing and forwarding (VRF) information for interfaces, use the **show vrf interface** command.

show vrf interface [**mgmt** *mgmt-number* | **vlan** *vlan-ID*]

Syntax Description

mgmt *mgmt-number*	(Optional) Displays the management interfaces that are added to a VRF. The management interface number is 0.
vlan *vlan-ID*	(Optional) Displays the VLAN interfaces that are added to a VRF. The VLAN interface range is from 1 to 4094.

Command Default

All interfaces

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the VRF information for all configured interfaces:

```
switch# show vrf interface
Interface                  VRF-Name                        VRF-ID
Vlan1                      default                              1
Vlan5                      default                              1
loopback1                  default                              1
mgmt0                      management                           2
switch#
```

This example shows how to display the VRF information for management interfaces:

```
switch# show vrf interface mgmt 0
Interface                  VRF-Name                        VRF-ID
mgmt0                      management                           2
switch#
```

This example shows how to display the VRF information for VLAN interfaces:

```
switch# show vrf interface vlan 1
Interface                  VRF-Name                        VRF-ID
Vlan1                      default                              1
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
vrf member	Adds an interface to a VRF.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

T Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with T.

Review Draft -- Cisco Confidential

template (BGP)

To create a peer template and enter a peer template configuration mode, use the **template** command. To remove a peer template, use the **no** form of this command.

template {**peer** *name* | **peer-policy** *name* | **peer-session** *name*}

no template {**peer** *name* | **peer-policy** *name* | **peer-session** *name*}

Syntax Description

peer *name*	Specifies the name of the neighbor template.
peer-policy *name*	Specifies the name of the peer-policy template.
peer-session *name*	Specifies the name of the peer-session template.

Command Default

This command has no default settings.

Command Modes

Neighbor address-family configuration mode
Router bgp configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **template** command allows you to enable a set of predefined attributes that a neighbor inherits.

Note A Border Gateway Protocol (BGP) neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong to a peer group or to inherit policies from peer templates only.

Peer templates support only general policy commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer templates.

When you enter the peer-policy template configuration mode, the following commands are available:

- **suppress-inactive**—Advertises the active routes to the peer only. See the **suppress-inactive** command for additional information.
- **exit**—Exits current configuration mode.
- **filter-list** *name* {**in** | **out**}—Creates the AS-PATH filter-list on the inbound and the outbound BGP routes. To remove the entry, use the **no** form of this command.
  - **in**—Applies the access list to incoming routes.
  - **out**—Applies the access list to outgoing routes.

Review Draft -- Cisco Confidential

- **inherit peer-policy** *policy-name seq-num*—Configures a peer-policy template to inherit the configuration from another peer-policy template. To remove an inherited statement from a peer-policy template, use the **no** form of this command. Range: 1 to 65535. Default: No inherit statements are configured.

  The sequence number specifies the order in which the peer policy template is evaluated. Like a route-map sequence number, the lowest sequence number is evaluated first. Peer policy templates support inheritance and a peer can directly and indirectly inherit up to seven peer policy templates. Inherited peer policy templates are configured with sequence numbers like route maps. An inherited peer policy template, like a route map, is evaluated starting with the inherit statement with the lowest sequence number. However, peer policy templates do not fall through. Every sequence is evaluated. If a BGP policy command is reapplied with a different value, it overwrites any previous value from a lower sequence number.

Note A Border Gateway Protocol (BGP) routing process cannot be configured to be a member of a peer group and to use peer templates for group configurations. You must use one method or the other. We recommend peer templates because they provide improved performance and scalability.

- **maximum-prefix** *max*—Specifies the maximum number of prefixes from this neighbor. Range: 1 to 300000. Default: This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. See the **maximum-prefix** command for additional information.
- **next-hop-self**—Configures the router as the next hop for a Border Gateway Protocol (BGP) neighbor or peer group. To disable this feature, use the **no** form of this command. Default: Disabled.
- **next-hop-third-party**—Computes a third-party next hop if possible.
- **no**—Negates a command or sets its defaults.
- **prefix-list** *name* {**in** | **out**}—Specifies the route type to apply the prefix list. To remove the entry, use the **no** form of this command.
  - **in**—Applies the prefix list to incoming routes.
  - **out**—Applies the prefix list to outgoing routes.
- **route-map** *name* {**in** | **out**}—Specifies the route map name to apply the route type to apply to the neighbor.
  - **in**—Applies the route map to incoming routes.
  - **out**—Applies the route map to outgoing routes.
- **route-reflector-client**—Configures the router as a BGP route reflector and configures the specified neighbor as its client. To indicate that the neighbor is not a client, use the **no** form of this command. Default: There is no route reflector in the autonomous system.

  By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, which prevents a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

  If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

  All the neighbors configured with this command are members of the client group and the remaining iBGP peers are members of the nonclient group for the local route reflector.

Review Draft -- Cisco Confidential

- **send-community**—Specifies that a community attribute be sent to a BGP neighbor. To remove the entry, use the **no** form of this command.
- **soft-reconfiguration**—Configures the Cisco NX-OS software to start storing updates. To not store received updates, use the **no** form of this command. Default: Disabled. Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

  To use soft reconfiguration, or a soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Clearing the BGP session using the **soft-reconfiguration** command has a negative effect on network operations and should only be used as a last resort.

  To determine whether a BGP router supports this capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message appears:

  "Received route refresh capability from peer."

  If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group inherit the characteristic configured with this command.

When you enter the peer-session template configuration mode, the following commands are available:

- **description** *description*—Configures a description to be displayed by the local or a peer router. You can enter up to 80 characters including spaces.
- **disable-connected-check**—Disables connection verification for eBGP peers no more than one hop away when the eBGP peer is configured with a loopback interface.
- **ebgp-multihop**—Accepts and attempts BGP connections to external peers that reside on networks that are not directly connected.

Note You should enter this command under the guidance of Cisco technical support staff only.

- **exit**—Exits current configuration mode.
- **inherit peer-session** *session-name*—Configures a peer-session template. To inherit the configuration from another peer-session template, use the **peer-session** keywords. To remove an inherit statement from a peer-session template, use the **no** form of this command.
- **local-as**—Allows you to customize the autonomous system number for eBGP peer groupings.
- **neighbor inherit peer-session**—Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
- **neighbor translate-update**—Upgrades a router running BGP in the NLRI format to support multiprotocol BGP.
- **password**—Enables MD5 authentication on a TCP connection between two BGP peers. The following configuration tools are available:
  - **0** *password*—Specifies an unencrypted neighbor password.
  - **3** *password*—Specifies an 3DES encrypted neighbor password
  - *password*—Specifies an unencrypted (cleartext) neighbor password
- **remote-private-as**—Removes the private AS number from outbound updates.
- **show ip bgp template peer-policy**—Displays the locally configured peer policy templates.
- **show ip bgp template peer-session**—Displays the locally configured peer session templates.
- **shutdown**—Disables a neighbor or peer group.

Review Draft -- Cisco Confidential

- **timers** *keepalive-time*—Configures keepalive and hold timers in seconds. Range: 0 to 3600. Default: 60.
- **update-source** {**ethernet** *mod/port* | **loopback** *virtual-interface* | **port-channel** *number*[**.***sub-interface*]}—Specifies the source of the BGP session and updates. Range: *virtual-interface* is 0 to 1023; *number* is 0 to 4096; (optional) **.***sub-interface* is 1 to 4093.

General session commands can be configured once in a peer-session template and then applied to many neighbors through the direct application of a peer-session template or through indirect inheritance from a peer-session template. The configuration of peer-session templates simplify the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to create a peer-session template named CORE1. This example inherits the configuration of the peer-session template named INTERNAL-BGP.

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# template peer-session CORE1
switch(config-router-stmp)#
```

This example shows how to create and configure a peer-policy template named CUSTOMER-A:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# template peer-policy CUSTOMER-A
switch(config-router-ptmp)# exit
switch(config-router)# route-map SET-COMMUNITY in
switch(config-router)# filter-list 20 in
switch(config-router)# inherit peer-policy PRIMARY-IN 20
switch(config-router)# inherit peer-policy GLOBAL 10
switch(config-router)# exit-peer-policy
switch(config-router)#
```

This example shows that the maximum prefixes that are accepted from the 192.168.1.1 neighbor is set to 1000:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router) network 192.168.0.0
switch(config-router)# maximum-prefix 1000
switch(config-router)#
```

This example shows that the maximum number of prefixes that are accepted from the 192.168.2.2 neighbor is set to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router) network 192.168.0.0
switch(config-router)# maximum-prefix 5000 50
switch(config-router)#
```

This example shows that the maximum number of prefixes that are accepted from the 192.168.3.3 neighbor is set to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router) network 192.168.0.0
```

Review Draft -- Cisco Confidential

```
switch(config-router)# neighbor 192.168.3.3 maximum-prefix 2000 restart 30
switch(config-router)#
```

This example shows that the warning messages are displayed when the maximum-prefix limit (500) for the 192.168.4.4 neighbor is exceeded:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# network 192.168.0.0
switch(config-router)# maximum-prefix 500 warning-only
switch(config-router)#
```

This example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# next-hop-self
switch(config-router)#
```

This example shows that the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# send-community
switch(config-router)#
```

This example shows that the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 multicast
switch(config-router-af)# send-community
switch(config-router-af)#
```

This example enables inbound soft reconfiguration for the neighbor 10.108.1.1. All the updates received from this neighbor are stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information is used to generate a new set of inbound updates.

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# soft-reconfiguration inbound
switch(config-router)#
```

Related Commands

Command	Description
address-family	Enters the address family mode for the Border Gateway Protocol (BGP).
password (BGP)	Configures a MD5 password for two BGP peers.
router bgp	Enters the assign an autonomous system (AS) number to a router and enters the router BGP configuration mode.

Review Draft -- Cisco Confidential

V Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with V.

Review Draft -- Cisco Confidential

vrf

To enter a virtual routing and forwarding (VRF) configuration mode and configure submode commands, use the **vrf** command. To remove a VRF instance or disable the VRF configuration mode, use the **no** form of this command.

vrf *name* | **management**

no vrf *name* | **management**

Syntax Description

name	Name of the VRF. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.
management	Specifies the management VRF.

Command Default

None

Command Modes

Address-family configuration mode
Router configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The VRF does not become active until you create an identically named VRF in global configuration mode.

When you enter the VRF configuration mode, the following commands are available:

- **area**—(OSPF) Configures area properties.
- **address-family**—(BGP) Configures an address-family. See the **address-family (BGP)** command for additional information.
- **auto-cost**—(OSPF) Calculates OSPF cost according to bandwidth.
- **cluster-id** {*cluster-id* | *cluster-ip-addr*}—(BGP) Configures the Route Reflector Cluster-ID (router, vrf). Range: 1 to 4294967295. You can enter the cluster identification as a 32-bit quantity or as an IP address. To remove the cluster ID, use the **no** form of this command. Together, a route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.

  The **cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors, which allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.

Review Draft -- Cisco Confidential

Note All route reflectors must maintain stable sessions between all peers in the cluster. If stable sessions cannot be maintained, you should use overlay route reflector clusters instead (route reflectors with different cluster IDs).

- **default-information**—(OSPF) Controls the distribution of the default route. See the **default-information originate (OSPF)** command for additional information.
- **default-metric**—(OSPF) Specifies the default metric for redistributed routes. See the **default-metric (OSPF)** command for additional information.
- **distance**—(OSPF) Defines the OSPF administrative distance. See the **distance (OSPF)** command for additional information.
- **exit**—(BGP) Exits from the current command mode.
- **log-adjacency-changes**—(OSPF) Logs changes in adjacency state.
- **log-neighbor-changes**—Enables logging of the BGP neighbor resets. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command. The **log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

  Using the **log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the internal buffer of the router, and are not stored to the disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

  The neighbor status change messages are not tracked if the bgp **log-neighbor-changes** command is disabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** command.

  The **eigrp log-neighbor-changes** command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the bgp **log-neighbor-changes** command.

  Use the **show logging command** to display the log for the BGP neighbor changes.
- **max-metric**—(OSPF) Maximizes the cost metric. See the **max-metric (OSPF)** command for additional information.
- **maximum-paths**—(OSPF) Sets the maximum number of parallel routes that OSPF can support. See the **maximum-paths (OSPF)** command for additional information.
- **neighbor**—Configures a BGP neighbor. See the **neighbor** command for additional information.
- **no**—Negates a command or set its defaults.
- **redistribute**—(OSPF) Redistributes information from another routing protocol. See the **redistribute (OSPF)** command for additional information.
- **rfc1583compatibility**—(OSPF) Configures RFSC 1583 compatibility for external path preferences. See the **rfc1583compatibility** command for additional information.
- **router-id** *ip-addr*—Specifies the IP address to use as the router-id.

Review Draft -- Cisco Confidential

- **shutdown**—(OSPF) Shuts down the OSPF protocol instance. See the **shutdown (OSPF)** command for additional information.
- **summary-address**—(OSPF) Configures route summarization for redistribution. See the **summary-address (OSPF)** command for additional information.
- **timers** *bestpath-timeout*—Configures the best-path timeout in seconds. Range: 1 to 3600. Default: 300.

Examples

This example shows how to enter VRF configuration mode in a BGP environment:

```
switch(config)# router bgp 100
switch(config-router)# vrf management
switch(config-router-vrf)#
```

This example shows how to enter VRF configuration mode in an OSPF environment:

```
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)# router ospf 201
switch(config-router)# vrf RemoteOfficeVRF
switch(config-router-vrf)#
```

Related Commands

Command	Description
vrf context	Creates a VRF.
show vrf	Displays the VRF configuration information.

Review Draft -- Cisco Confidential

vrf context

To create a virtual routing and forwarding instance (VRF) and enter VRF configuration mode, use the **vrf context** command. To remove a VRF entry, use the **no** form of this command.

vrf context {*name* | **management**}

no vrf context {*name* | **management**}

Syntax Description

name	Name of the VRF. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.
management	Specifies the management VRF.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to create a VRF context:

```
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)#
```

Related Commands

Command	Description
vrf	Creates or configures a VRF instance.
show vrf	Displays the VRF configuration information.

Review Draft -- Cisco Confidential

vrf member

To add an interface to a virtual routing and forwarding (VRF) instance or to configure object tracking on a VRF instance, use the **vrf member** command. To remove the object tracking for this route, use the **no** form of this command.

vrf member *vrf-name*

no vrf member *vrf-name*

Syntax Description

vrf-name	VRF name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Interface configuration mode
Object tracking confiuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **vrf member** command in object tracking configuration mode to track objects in a nondefault VRF.

Examples

This example shows how to track an IP route in VRF Red:

```
switch(config)# track 1 ip route 10.10.10.0/8 reachability
switch(config-track)# vrf member Red
switch(config-track)#
```

This example shows how to add the Ethernet interface 1/5 to VRF RemoteOfficeVRF:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)#
```

Related Commands

Command	Description
show vrf	Displays the VRF configuration information.

<l_Italic>Review Draft -- Cisco Confidential

PART 2

EIGRP Commands

Review Draft -- Cisco Confidential

A Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with A.

Review Draft -- Cisco Confidential

address-family (EIGRP)

To configure an address family for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **address-family** command. To remove an address family, use the **no** form of this command.

address-family ipv4 unicast

no address-family ipv4 unicast

Syntax Description

ipv4	Specifies the IPv4 address family.
unicast	Specifies unicast address support.

Command Default

None

Command Modes

Address-family configuration mode
Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to set the IPv4 unicast address family for an EIGRP instance:

```
switch(config)# router eigrp 201
switch(config-router)# address-family ipv4 unicast
switch(config-router)#
```

Related Commands

Command	Description
default-information	Controls the distribution of a default route.
default-metric	Configures the default metric for routes redistributed into EIGRP.
distance	Configures the administrative distance.
maximum-paths	Configures the maximum number of equal-cost paths.
redistribute	Configures route redistribution for EIGRP.
router-id	Configures the router ID.
show ip eigrp	Displays EIGRP information.
timers	Configures the EIGRP timers.

Review Draft -- Cisco Confidential

authentication key-chain (EIGRP)

To enable authentication for the Enhanced Interior Gateway Routing Protocol (EIGRP) packets and to specify the set of keys that can be used on an interface, use the **authentication key-chain** command. To prevent authentication, use the **no** form of this command.

authentication key-chain *name-of-chain*

no authentication key-chain *name-of-chain*

Syntax Description

name-of-chain	Group of keys that are valid.

Command Default

No authentication is provided for EIGRP packets.

Command Modes

Address-family configuration mode
Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Set the authentication mode using the **authentication mode** command in VRF configuration mode. You must separately configure a key chain using the **key-chain** command to complete the authentication configuration for an interface.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the interface to accept and send any key that belongs to the key-chain trees:

```
switch(config)# router eigrp 209
switch(config-router)# vrf red
switch(config-router-vrf)# authentication key-chain trees
```

Related Commands

Command	Description
authentication mode (EIGRP)	Sets the authentication mode for EIGRP in a VRF.
ip authentication key-chain eigrp	Enables authentication for EIGRP and specifies the set of keys that can be used on an interface.
key-chain	Creates a set of keys that can be used by an authentication method.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

authentication mode (EIGRP)

To specify the type of authentication used in the Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the **authentication mode** command. To remove authentication, use the **no** form of this command.

authentication mode md5

no authentication mode md5

Syntax Description

md5	Specifies Message Digest 5 (MD5) authentication.

Command Default

None

Command Modes

Address-family configuration mode
Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure the interface to use MD5 authentication:

```
switch(config)# router eigrp 209
switch(config-router)# vrf red
switch(config-router-vrf)# authentication mode md5
switch(config-router-vrf)#
```

Related Commands

Command	Description
authentication key-chain eigrp	Enables authentication for EIGRP and specifies the set of keys that can be used on an interface.
ip authentication mode eigrp	Configures the authentication mode for EIGRP on an interface.
key chain	Creates a set of keys that can be used by an authentication method.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

autonomous-system

To configure the autonomous system (AS) number for an Enhanced Interior Gateway Routing Protocol (EIGRP) address family, use the **autonomous-system** command. To revert to default, use the **no** form of this command.

autonomous-system *as-number*

no autonomous-system [*as-number*]

Syntax Description

as-number	Autonomous system number. The range is from 1 to 65535.

Command Default

None

Command Modes

Address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **autonomous-system** command to set a common AS number for all EIGRP instances in an address family.

This command requires the LAN Base Services license.

Examples

This example shows how to set an AS number for EIGRP for IPv4 unicast:

```
switch(config)# router eigrp 201
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# autonomous-system 64496
switch(config-router-af)#
```

Related Commands

Command	Description
address-family (EIGRP)	Enters the address family configuration mode for EIGRP.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with C.

Review Draft -- Cisco Confidential

clear ip eigrp accounting

To clear the prefix accounting information for the Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the **clear ip eigrp accounting** command.

clear ip eigrp accounting [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
all	(Optional) Clears the EIGRP accounting information from all VRF instances.
default	(Optional) Clears the EIGRP accounting information from the default VRF.
management	(Optional) Clears the EIGRP accounting information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear the EIGRP accounting information:

```
switch# clear ip eigrp accounting
```

Review Draft -- Cisco Confidential

clear ip eigrp neighbors

To remove and reestablish the Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor entries from the appropriate table, use the **clear ip eigrp neighbors** command.

clear ip eigrp neighbors [* | *ip-address* | **ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*] [**soft**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

*	(Optional) Clears all neighbors.
ip-address	(Optional) Address of the neighbor.
ethernet *slot/port*	(Optional) Clears the Ethernet interface from the neighbor table. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Clears the loopback interface from the neighbor table. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Clears the EtherChannel interface and EtherChannel number from the neighbor table. The range is from 1 to 4096.
soft	(Optional) Specifies soft reset for the neighbors.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.
all	(Optional) Clears the EIGRP neighbor information from all VRF instances.
default	(Optional) Clears the EIGRP neighbor information from the default VRF.
management	(Optional) Clears the EIGRP neighbor information from the management VRF.

Command Default

When no autonomous system number, interface, or VRF instance is specified, all EIGRP neighbor entries are cleared from the table.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear all EIGRP entries for neighbors on Ethernet interface 2/1:

```
switch# clear ip eigrp vrf * neighbors ethernet 2/1
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip eigrp interfaces	Displays information about interfaces configured for EIGRP.
show ip eigrp neighbors	Displays the neighbors discovered by EIGRP.

Review Draft -- Cisco Confidential

clear ip eigrp redistribution

To clear redistribution information for the Enhanced Interior Gateway Routing Protocol (EIGRP) , use the **clear ip eigrp redistribution** command.

clear ip eigrp redistribution [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is a case-sensitive, alphanumeric string of up to 32 characters.
all	(Optional) Clears the redistribution information from all VRF instances.
default	(Optional) Clears the redistribution information from the default VRF.
management	(Optional) Clears the redistribution information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear redistribution information:

```
switch# clear ip eigrp redistribution
```

Related Commands

Command	Description
feature eigrp	Enables the EIGRP feature.

Review Draft -- Cisco Confidential

clear ip eigrp traffic

To clear the Enhanced Interior Gateway Routing Protocol (EIGRP) traffic statistics, use the **clear ip eigrp traffic** command.

clear ip eigrp traffic [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Clears the traffic statistics from all VRF instances.
default	(Optional) Clears the traffic statistics from the default VRF.
management	(Optional) Clears the traffic statistics from the management VRF.

Command Default

This command clears information for the default VRF if no VRF is specified.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear the EIGRP traffic statistics:

```
switch# clear ip eigrp traffic
```

Review Draft -- Cisco Confidential

D Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with D.

Review Draft -- Cisco Confidential

default-information originate (EIGRP)

To generate a default route into the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-information originate** command. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**route-map** *map-name*]

no default-information originate

Syntax Description

always	(Optional) Generates the default route if the route is not in the EIGRP routing information base.
route-map *map-name*	(Optional) Generates the default route only if the route is permitted by the route map. The map name is an alphanumeric string of up to 63 characters.

Command Default

Disabled

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to originate a default route (0.0.0.0/0) to all routes that pass the Condition route map:

```
switch(config)# router eigrp 201
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# default-information originate route-map Condition
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
default-metric	Sets the metric for routes redistributed into EIGRP.
redistribute	Redistributes routes from other routing protocols into EIGRP.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

default-metric (EIGRP)

To set metrics for an Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-metric** command. To remove the metric value and restore the default state, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric

Syntax Description

bandwidth	Minimum bandwidth of the route in kilobits per second. The range is from 1 to 16777215. The default value is 100000.
delay	Route delay in tens of microseconds. The range is from 1 to 16777215. The default value is 100 (tens of microseconds).
reliability	Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100-percent reliability; 0 means no reliability. The default value is 255.
loading	Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100-percent loading). The default value is 1.
mtu	Minimum maximum transmission unit (MTU) size of the route in bytes. The range is from 128 to 4352.

Command Default

bandwidth: 100000

delay: 100 (tens of microseconds)

reliability: 255

loading: 1

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **default-metric** command with the **redistribute** command to use the same metric value for all redistributed routes. A default metric helps to solve the problem of redistributing routes with incompatible metrics. Whenever external metrics do not convert to EIGRP metrics, you can use a default metric to provide a reasonable substitute to the external metric and enable the redistribution to proceed.

This command requires the LAN Base Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to take redistributed Routing Information Protocol (RIP) metrics and translate them into EIGRP metrics with the following values: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
switch(config)# router eigrp 1
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute rip 100 route-map FilterRIP
switch(config-router-af)# default-metric 1000 100 250 100 1500
switch(config-router-af)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
redistribute	Redistributes routes from one routing domain into another routing domain.
show ip eigrp route-map statistics redistribute	Displays information about EIGRP route map statistics.

Review Draft -- Cisco Confidential

distance (EIGRP)

To allow the use of two administrative distances (internal and external) for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the **distance** command. To return to the default setting, use the **no** form of this command.

distance *internal-distance external-distance*

no distance

Syntax Description

internal-distance	Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.
external-distance	Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.

Command Default

internal-distance: 90
external-distance: 170

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, a higher value indicates a lower trust rating. An administrative distance of 255 means that the routing information source cannot be trusted and should be ignored.

Use the **distance** command if another protocol is known to provide a better route to a node than was actually learned through the external EIGRP or some internal routes should be preferred by EIGRP.

This command requires the LAN Base Services license.

Examples

This example shows how to set the administrative distance of all EIGRP 1 internal routes to 80 and all EIGRP external routes to 130:

```
switch(config)# router eigrp 1
switch(config-router)# distance 80 130
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

E Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with E.

Review Draft -- Cisco Confidential

eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **eigrp log-neighbor-changes** command. To disable the logging of changes in EIGRP neighbor adjacencies, use the **no** form of this command.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **eigrp log-neighbor-changes** command to log neighbor adjacency changes to monitor the stability of the routing system and to detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the **no** form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to enable logging of neighbor changes for EIGRP process 209:

```
switch(config)# router eigrp 209
switch(config-router)# eigrp log-neighbor-changes
```

Related Commands

Command	Description
log-adjacency-changes	Enables logging of EIGRP adjacency state changes.
log-neighbor-changes	Enables logging of EIGRP neighbor changes.
log-neighbor-warnings	Enables logging of EIGRP neighbor warnings.

Review Draft -- Cisco Confidential

eigrp log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** command. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) Time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 to 65535.

Command Default

Neighbor warning messages are logged.

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **eigrp log-neighbor-warnings** command to enable neighbor warning messages and to configure the interval between repeated neighbor warning messages.

This command requires the LAN Base Services license.

Examples

This example shows how to log neighbor warning messages for EIGRP process 209 and to repeat the warning messages in 5-minute (300 seconds) intervals:

```
switch(config)# router eigrp 209
switch(config-router)# eigrp log-neighbor-warnings 30
```

Related Commands

Command	Description
log-adjacency-changes	Enables logging of EIGRP adjacency state changes.
log-neighbor-changes	Enables logging of EIGRP neighbor changes.
log-neighbor-warnings	Enables logging of EIGRP neighbor warnings.

Review Draft -- Cisco Confidential

eigrp router-id

To set the router ID used by the Enhanced Interior Gateway Routing Protocol (EIGRP) when communicating with its neighbors, use the **eigrp router-id** command. To remove the configured router ID, use the **no** form of this command.

eigrp router-id *ip-address*

no eigrp router-id *ip-address*

Syntax Description

ip-address	Router ID in dotted decimal notation.

Command Default

EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started.

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest local IP address is selected and loopback interfaces are preferred. The router ID is not changed unless the EIGRP process is removed with the **no router eigrp** command or if the router ID is manually configured with the **eigrp router-id** command.

Use the **eigrp router-id** command to manually configure the router ID for EIGRP. The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. The router ID can be configured with any IP address with two exceptions; 0.0.0.0 and 255.255.255.255 are not legal values and cannot be entered. You should configure a unique value for each router.

This command requires the LAN Base Services license.

Examples

This example shows how to configure 172.16.1.3 as a fixed router ID:

```
switch(config)# router eigrp 209
switch(config-router)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
show ip eigrp	Displays a summary of the EIGRP processes.

Review Draft -- Cisco Confidential

eigrp stub

To configure a router as a stub using the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **eigrp stub** command. To disable the EIGRP stub routing feature, use the **no** form of this command.

eigrp stub [**direct** | **leak-map** *map-name* | **receive-only** | **redistributed**]

no eigrp stub [**direct** | **leak-map** *map-name* | **receive-only** | **redistributed**]

Syntax Description

direct	(Optional) Advertises directly connected routes.
leak-map *map-name*	(Optional) Allows dynamic prefixes based on the leak map.
receive-only	(Optional) Sets the router as a receive-only neighbor.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.

Command Default

Disabled

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **eigrp stub** command to configure a router as a stub where the router directs all IP traffic to a distribution router.

The **direct** keyword permits EIGRP stub routing to advertise connected routes. This option is enabled by default.

The **receive-only** keyword restricts the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword does not permit any other option to be specified because it prevents any type of route from being sent.

The **redistributed** keyword permits the EIGRP Stub Routing feature to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP does not advertise redistributed routes.

If you use any of these four keywords (**direct**, **leak-map**, **receive-only**, **redistributed**) with the **eigrp stub** command, only the route types specified by the particular keyword are advertised.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the router as a receive-only neighbor:

```
switch(config)# router eigrp 1
```

Review Draft -- Cisco Confidential

```
switch(config-router)# eigrp stub receive-only
```

Related Commands

Command	Description
show ip eigrp	Displays a summary of the EIGRP processes.

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with F.

Review Draft -- Cisco Confidential

feature eigrp

To enable the Enhanced Interior Gateway Protocol (EIGRP), use the **feature eigrp** command. To disable EIGRP, use the **no** form of this command.

feature eigrp

no feature eigrp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the EIGRP feature before you can configure EIGRP.

This command requires the LAN Base Services license.

Examples

This example shows how to enable the EIGRP feature:

```
switch# configure terminal
switch(config)# feature eigrp
switch(config)#
```

This example shows how to disable the EIGRP feature:

```
switch# configure terminal
switch(config)# no feature eigrp
switch(config)#
```

Related Commands

Command	Description
router eigrp	Creates a EIGRP instance.
show feature	Displays the features enabled on the switch.
show ip eigrp	Displays EIGRP configuration information.

Review Draft -- Cisco Confidential

flush-routes (EIGRP)

To flush all EIGRP routes in the unicast RIB when an EIGRP instance restarts, use the **flush-routes** command. To disable this feature, use the **no** form of this command.

flush-routes

no flush-routes

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to flush routes when an EIGRP instance restarts:

```
switch(config)# router eigrp Test1
switch(config-router)# flush-routes
switch(config-router)#
```

Related Commands

Command	Description
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with I.

Review Draft -- Cisco Confidential

ip authentication key-chain eigrp

To enable authentication for the Enhanced Interior Gateway Routing Protocol (EIGRP) packets and to specify the set of keys that can be used on an interface, use the **ip authentication key-chain eigrp** command. To prevent authentication, use the **no** form of this command.

ip authentication key-chain eigrp *instance-tag name-of-chain*

no ip authentication key-chain eigrp *instance-tag name-of-chain*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
name-of-chain	Group of keys that are valid.

Command Default

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must set the authentication mode using the **ip authentication mode eigrp** command in interface configuration mode. You must separately configure a key chain using the **key-chain** command to complete the authentication configuration for an interface.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the interface to accept and send any key that belongs to the key-chain trees:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip authentication key-chain eigrp 209 trees
switch(config-if)#
```

Related Commands

Command	Description
ip authentication mode eigrp	Sets the authentication mode for EIGRP on an interface.
key-chain	Creates a set of keys that can be used by an authentication method.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

ip authentication mode eigrp

To specify the type of authentication used in the Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the **ip authentication mode eigrp** command. To remove authentication, use the **no** form of this command.

ip authentication mode eigrp *instance-tag* **md5**

no ip authentication mode eigrp *instance-tag* **md5**

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
md5	Specifies Message Digest 5 (MD5) authentication.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure the interface to use MD5 authentication:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip authentication mode eigrp 209 md5
switch(config-if)#
```

Related Commands

Command	Description
authentication mode (EIGRP)	Configures the authentication mode for EIGRP in a VRF.
copy running-config startup-config	Copies the configuration changes to the startup configuration file.
ip authentication key-chain eigrp	Enables authentication for EIGRP and specifies the set of keys that can be used on an interface.
key chain	Creates a set of keys that can be used by an authentication method.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

ip bandwidth eigrp

To configure the bandwidth metric on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip bandwidth eigrp** command. To restore the default, use the **no** form of this command.

ip bandwidth eigrp *instance-tag bandwidth*

no ip bandwidth eigrp

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
bandwidth	Bandwidth value. The range is from 1 to 2,560,000,000 kilobits.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure EIGRP to use a bandwidth metric of 10000 in autonomous system 209:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip bandwidth eigrp 209 10000
```

Related Commands

Command	Description
ip bandwidth-percent eigrp	Sets the percent of the interface bandwidth that EIGRP can use.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip bandwidth-percent eigrp** command. To restore the default, use the **no** form of this command.

ip bandwidth-percent eigrp *instance-tag percent*

no ip bandwidth-percent eigrp

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
percent	Percentage of bandwidth that EIGRP may use.

Command Default

percent: 50

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

EIGRP uses up to 50 percent of the bandwidth of a link, as defined by the **ip bandwidth** interface configuration command. Use the **ip bandwidth-percent** command to change this default percent.

This command requires the LAN Base Services license.

Examples

This example shows how to configure EIGRP to use up to 75 percent of an interface in autonomous system 209:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip bandwidth-percent eigrp 209 75
switch(config-if)#
```

Related Commands

Command	Description
ip bandwidth eigrp	Sets the EIGRP bandwidth value for an interface.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip delay eigrp

To configure the throughput delay for the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip delay eigrp** command. To restore the default, use the **no** form of this command.

ip delay eigrp *instance-tag seconds*

no ip delay eigrp instance-tag

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
seconds	Throughput delay, in tens of microseconds. The range is from 1 to 16777215.

Command Default

100 (10-microsecond units)

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You configure the throughput delay on an interface in 10-microsecond units. For example, if you set the **ip delay eigrp** command to 100, the throughput delay is 1000 microseconds.

This command requires the LAN Base Services license.

Examples

This example shows how to set the delay to 400 microseconds for the interface:

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip delay eigrp 1 40
```

Related Commands

Command	Description
ip hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process that is designated by an autonomous system number.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip distribute-list eigrp

To configure a distribution list for the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip distribute-list eigrp** command. To restore the default, use the **no** form of this command.

ip distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

no ip distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
prefix-list *list-name*	Specifies the name of an IP prefix list to filter EIGRP routes.
route-map *map-name*	Specifies the name of a route map to filter EIGRP routes.
in	Applies the route policy to incoming routes.
out	Applies the route policy to outgoing routes.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip distribute-list eigrp** command to configure a route filter policy on an interface. You must configure the named route map or prefix list to complete this configuration.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a route map for all EIGRP routes coming into the interface:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip distribute-list eigrp 209 route-map InputFilter in
switch(config-if)#
```

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.
show ip eigrp	Displays EIGRP information

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

ip eigrp shutdown

To shut down the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip eigrp shutdown** command. To restore the default, use the **no** form of this command.

ip eigrp *instance-tag* **shutdown**

no ip eigrp *instance-tag* **shutdown**

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip eigrp shutdown** command to shut down the interface for EIGRP and prevent EIGRP adjacency for the interface for maintenance purposes. The network address for the interface does not show up in the EIGRP topology table.

Use the **ip passive-interface eigrp** command to prevent EIGRP adjacency but keep the network address in the topology table.

This command requires the LAN Base Services license.

Examples

This example shows how to disable EIGRP on an interface:

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip eigrp 201 shutdown
```

Related Commands

Command	Description
ip passive-interface eigrp	Configures an instance of EIGRP.
router eigrp	Configures an instance of EIGRP.

Review Draft -- Cisco Confidential

ip hello-interval eigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) hello interval for an interface, use the **ip hello-interval eigrp** command. To restore the default, use the **no** form of this command.

ip hello-interval eigrp *instance-tag seconds*

no ip hello-interval eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
seconds	Hello interval (in seconds). The range is from 1 to 65535.

Command Default

5 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to set the hello interval to 10 seconds for the interface:

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip hello-interval eigrp 1 10
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip hold-time eigrp

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip hold-time eigrp** command. To restore the default, use the **no** form of this command.

ip hold-time eigrp *instance-tag seconds*

no ip hold-time eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
seconds	Hold time (in seconds). The range is from 1 to 65535.

Command Default

15 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip hold-time eigrp** command to increase the default hold time on very congested and large networks.

We recommend that you configure the hold time to be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

This command requires the LAN Base Services license.

Examples

This example shows how to set the hold time to 40 seconds for the interface:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip hold-time eigrp 209 40
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.

Review Draft -- Cisco Confidential

Command	Description
ip hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process designated by an autonomous system number.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip next-hop-self eigrp

To instruct the Enhanced Interior Gateway Routing Protocol (EIGRP) process to use the local IP address as the next-hop address when advertising these routes, use the **ip next-hop-self eigrp** command. To use the received next-hop value, use the **no** form of this command.

ip next-hop-self eigrp *instance-tag*

no ip next-hop-self eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

EIGRP always sets the IP next-hop value to be itself.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

EIGRP, by default, sets the IP next-hop value to be itself for routes that it is advertising, even when advertising those routes on the same interface from which the router learned them. To change this default, you must use the **no ip next-hop-self eigrp** command to instruct EIGRP to use the received next-hop value when advertising these routes.

Examples

This example shows how to change the default IP next-hop value and instruct EIGRP to use the received next-hop value:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# no ip next-hop-self eigrp 209
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip offset-list eigrp

To configure an offset list for the Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip offset-list eigrp** command. To restore the default, use the **no** form of this command.

ip offset-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

no ip offset-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
prefix-list *list-name*	Specifies the name of an IP prefix list to filter EIGRP routes.
route-map *map-name*	Specifies the name of a route map to filter EIGRP routes.
in	Applies the route policy to incoming routes.
out	Applies the route policy to outgoing routes.
offset	Value to add to the EIGRP metric. The range is from 0 to 2147483647.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Cisco Nexus 6000 adds the configured offset value to any routes that match the configure prefix list or route map. You must configure the named route map or prefix list to complete this configuration.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an offset list filter to add 20 to the metric for EIGRP routes coming into the interface that match the route map OffsetFilter:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip offset-list eigrp 209 route-map OffsetFilter in 20
switch(config-if)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip passive-interface eigrp

To suppress all routing updates on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip passive-interface eigrp** command. To reenable the sending of routing updates, use the **no** form of this command.

ip passive-interface eigrp *instance-tag*

no ip passive-interface eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The name can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

Routing updates are sent on the interface.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip passive-interface eigrp** command to stop all routing updates on an interface and suppress the formation of EIGRP adjacencies. The network address for the interface remains in the EIGRP topology table.

This command requires the LAN Base Services license.

Examples

This example shows how to stop EIGRP routing updates on ethernet 2/1:

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip passive-interface eigrp 201
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration in the startup configuration file.
no switchport	Configures an interface as a Layer 3 routed interface.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

ip route

To configure a static route, use the **ip route** command. To remove the static route, use the **no** form of this command.

ip route *ip-prefix/mask* {[*interface*] *next-hop*} [*preference*] [**tag** *id*]

no ip route *ip-prefix/mask* {[*interface*] *next-hop*} [*preference*] [**tag** *id*]

Syntax Description

ip-prefix/mask	IP prefix and prefix mask. The format is x.x.x.x/length. The length is 1 to 32.
interface	(Optional) Interface on which all packets are sent to reach this route. Use **?** to display a list of supported interfaces.
next-hop	IP address of the next hop that can be used to reach that network. You can specify an IP address and an interface type and interface number. The format is x.x.x.x/length. The length is 1 to 32.
preference	(Optional) Route preference that is used as the administrative distance to this route. The range is from 1 to 255. The default is 1.
tag *id*	(Optional) Assigns a route tag that can be used to match against in a route map. The range is from 0 to 4294967295. The default is 0.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Static routes have a default administrative distance of 1. If you want a dynamic routing protocol to take precidence over a static route, you must configure the static route preference argument to be greater than the administrative distance of the dynamic routing protocol. For example, routes derived with the Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, you should specify an administrative distance greater than 100.

Examples

This example shows how to create a static route for destinations with the IP address prefix 192.168.1.1/32, reachable through the next-hop address 10.0.0.2:

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2
```

This example shows how to assign a tag to the previous example so that you can configure a route map that can match on this static route:

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2 tag 5
```

Review Draft -- Cisco Confidential

This example shows how to choose a preference of 110. In this case, packets for prefix 10.0.0.0 are routed to a router at 172.31.3.4 if dynamic route information with an administrative distance less than 110 is not available.

```
switch# configure terminal
switch(config)# ip route 10.0.0.0/8 172.31.3.4 110
switch(config)#
```

Related Commands

Command	Description
show vrf	Displays the VRF configuration information.

Review Draft -- Cisco Confidential

ip router eigrp

To specify the Enhanced Interior Gateway Routing Protocol (EIGRP) instance for an interface, use the **ip router eigrp** command. To return to the default, use the **no** form of this command.

ip router eigrp *instance-tag*

no ip router eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, make sure that you enable EIGRP on the switch.

This command requires the LAN Base Services license.

Examples

This example shows how to set the EIGRP instance for an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router eigrp Base
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes in the startup configuration file.
feature eigrp	Enables EIGRP on the switch.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

ip split-horizon eigrp

To enable split horizon for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **ip split-horizon eigrp** command. To disable split horizon, use the **no** form of this command.

ip split-horizon eigrp *instance-tag*

no ip split-horizon eigrp *instance-tag*

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

Enabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **no ip split-horizon eigrp** command to disable split horizon on an interface.

This command requires the LAN Base Services license.

Examples

This example shows how to disable split horizon an an Ethernet link:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# no ip split-horizon eigrp 209
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

ip summary-address eigrp

To configure a summary aggregate address for the specified Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip summary-address eigrp** command. To disable a configuration, use the **no** form of this command.

ip summary-address eigrp *instance-tag* {*ip-address/length* | *ip-address mask*} [*admin-distance* | **leak-map** *map-name*]

no ip summary-address eigrp *instance-tag* {*ip-address/length* | *ip-address mask*}

Syntax Description

instance-tag	Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.
ip-address/length	Summary IP prefix and prefix length to apply to an interface in four-part, dotted-decimal notation. For example, /8 indicates that the first eight bits in the IP prefix are network bits. If *length* is used, the slash is required.
ip-address	Summary IP address to apply to an interface in four-part, dotted-decimal notation.
mask	IP address mask.
admin-distance	(Optional) Administrative distance. The range is from 1 to 255.
leak-map *map-name*	(Optional) Specifies the leak map.

Command Default

An administrative distance of 5 is applied to EIGRP summary routes.
No summary addresses are predefined.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip summary-address eigrp** command to configure interface-level address summarization. EIGRP summary routes are given an administrative distance of 5.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an administrative distance of 95 on an EIGRP interface for the 192.168.0.0/16 summary address:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip summary-address eigrp 209 192.168.0.0/16 95
switch(config-if)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp interfaces	Displays EIGRP interface-related information.

Review Draft -- Cisco Confidential

L Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with L.

Review Draft -- Cisco Confidential

log-adjacency-changes (EIGRP)

To enable the logging of changes in the Enhanced Interior Gateway Routing Protocol (EIGRP) adjacency state, use the **log-adjacency-changes** command. To disable the logging of changes in the EIGRP adjacency state, use the **no** form of this command.

log-adjacency-changes

no log-adjacency-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are not logged.

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to enable logging of adjacency state changes for EIGRP 1:

```
switch(config)# router eigrp 1
switch(config-router)# address-family ipv4
switch(config-router-af)# log-adjacency-changes
switch(config-router-af)#
```

Related Commands

Command	Description
ip eigrp log-neighbor-changes	Logs changes to neighbors for an interface.
ip eigrp log-neighbor-warnings	Logs neighbor warnings for an interface.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **log-neighbor-warnings** command. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

log-neighbor-warnings [*seconds*]

no log-neighbor-warnings [*seconds*]

Syntax Description

seconds	(Optional) Time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 to 65535.

Command Default

Neighbor warning messages are logged.

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **log-neighbor-warnings** command to enable neighbor warning messages and to configure the interval between repeated neighbor warning messages.

This command requires the LAN Base Services license.

Examples

This example shows how to log neighbor warning messages for EIGRP process 209 and to repeat the warning messages in 5-minute (300 seconds) intervals:

```
switch(config)# router eigrp 209
switch(config-router)# log-neighbor-warnings 30
switch(config-router)#
```

Related Commands

Command	Description
log-adjacency-changes	Enables logging of EIGRP adjacency state changes.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

M Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with M.

Review Draft -- Cisco Confidential

maximum-paths (EIGRP)

To control the maximum number of parallel routes that the Enhanced Interior Gateway Routing Protocol (EIGRP) can support, use the **maximum-paths** command. To remove the **maximum-paths** command from the configuration file and restore the default, use the **no** form of this command.

maximum-paths *maximum*

no maximum- paths

Syntax Description

maximum	Maximum number of parallel routes that EIGRP can install in a routing table. The range is from 1 to 16 routes.

Command Default

8 paths

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **maximum-paths** command to allow EIGRP to install multiple paths into the routing table for each prefix. Multiple paths are installed for both internal and external routes that are learned in the same autonomous system and that have an equal cost (according to the EIGRP best path algorithm).

This command requires the LAN Base Services license.

Examples

This example shows how to allow a maximum of 10 paths to a destination:

```
switch(config)# router eigrp 1
switch(config-router)# maximum-paths 10
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

metric maximum-hops

To advertise that those Enhanced Interior Gateway Routing Protocol (EIGRP) routes with a higher hop count than you specified are unreachable, use the **metric maximum-hops** command. To reset the value to the default, use the **no** form of this command.

metric maximum-hops *hops-number*

no metric maximum-hops

Syntax Description

hops-number	Maximum hop count. The range is from 1 to 255 hops.

Command Default

hops-number: 100

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **metric maximum-hops** command to provide a safety mechanism that causes EIGRP to advertise routes with a hop count greater than the value assigned to the *hops-number* argument as unreachable.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a hop count to 200:

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# metric maximum-hops 200
switch(config-router-af)#
```

Related Commands

Command	Description
metric weights	Tunes the EIGRP metric calculations.

Review Draft -- Cisco Confidential

metric weights

To tune the Enhanced Interior Gateway Routing Protocol (EIGRP) metric calculations, use the **metric weights** command. To reset the values to their defaults, use the **no** form of this command.

metric weights *tos k1 k2 k3 k4 k5*

no metric weights

Syntax Description

tos	Type of service (ToS). The range is from 0 to 8.
k1 k2 k3 k4 k5	Constants that convert an EIGRP metric vector into a scalar quantity. The arguments are as follows: • k1—The range is from 0 to 255. The default is 1. • k2—The range is from 0 to 255. The default is 0. • k3—The range is from 1 to 255. The default is 1. • k4—The range is from 0 to 255. The default is 0. • k5—The range is from 0 to 255. The default is 0.

Command Default

tos: 0

k1: 1

k2: 0

k3: 1

k4: 0

k5: 0

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **metric weights** command to alter the default behavior of EIGRP routing and metric computation and allow the tuning of the EIGRP metric calculation for a particular type of service (ToS).

This command requires the LAN Base Services license.

Examples

This example shows how to set the metric weights to change the default values:

```
switch(config)# router eigrp 1
```

Review Draft -- Cisco Confidential

```
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# metric weights 0 2 0 2 0 0
switch(config-router-af)#
```

Related Commands

Command	Description
bandwidth	Sets the EIGRP bandwidth metric in interface configuration mode.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
delay	Sets the EIGRP delay metric in interface configuration mode.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

R Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with R.

Review Draft -- Cisco Confidential

redistribute (EIGRP)

To inject routes from one routing domain into the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **redistribute** command. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

redistribute {**bgp** *as-number* | **direct** | **eigrp** *id* | **ospf** *instance-tag* | **rip** *instance-tag* | **static**} [**route-map** *map-name*]

no redistribute {**bgp** *as-number* | **direct** | **eigrp** *as-number* | **ospf** *instance-tag* | **rip** *instance-tag* | **static**}

Syntax Description

bgp *as-number*	Distributes routes from Border Gateway Protocol (BGP). The *as-number* is a 2-byte or 4-byte autonomous system number. The range for 2-byte numbers is from 1 to 65535. The range for 4-byte numbers is from 1.0 to 65535.65535.
direct	Distributes routes that are directly connected on an interface.
eigrp *id*	Specifies the name of an EIGRP instance. The *id* can be any case-sensitive, alphanumeric string up to 20 characters.
ospf *instance-tag*	Distributes routes from the OSPF protocol. This protocol is supported in the IPv4 address family. The *instance-tag* can be a maximum of 20 alphanumeric characters.
rip *instance-tag*	Distributes routes from the RIP protocol. The *instance-tag* can be a maximum of 20 alphanumeric characters.
static	Redistributes IP static routes.
route-map *map-name*	(Optional) Specifies the identifier of a configured route map. Use a route map to filter which routes are redistributed into EIGRP.

Command Default

Disabled

Command Modes

Address family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **redistribute** command to import routes from other routing protocols into EIGRP. You should always use a route map to filter these routes to ensure that EIGRP redistributes only the routes that you intend to redistribute.

Review Draft -- Cisco Confidential

You must configure a default metric to redistribute routes from another protocol into EIGRP. You can configure the default metric with the **default-metric** command or with the route map configured with the **redistribute** command.

This command requires the LAN Base Services license.

Examples

This example shows how to redistribute cause BGP routes into an EIGRP autonomous system:

```
switch(config)# router eigrp 209
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# redistribute bgp 64496
switch(config-router-af)
```

Related Commands

Command	Description
default-metric (EIGRP)	Sets the default metrics for routes redistributed into EIGRP.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

redistribute maximum-prefix (EIGRP)

To limit the number of routes redistributed into Enhanced Interior Gateway Routing Protocol (EIGRP), use the **redistribute maximum-prefix** command. To return to the default setting, use the **no** form of this command.

redistribute maximum-prefix *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]]

no redistribute maximum-prefix *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]

Syntax Description

max	Maximum number of prefixes that EIGRP will distribute. The range is from 0 to 65536.
threshold	(Optional) Percentage of maximum prefixes that triggers a warning message. The range is from 1 to 100. The default is 75 percent.
warning-only	(Optional) Logs a warning message when the maximum number of prefixes is exceeded.
widthdraw	(Optional) Withdraws all redistributed routes.
num-retries	(Optional) Number of times EIGRP tries to retrieve the redistributed routes. The range is from 1 to 12. The default is 1.
timeout	(Optional) Time between retry attempts. The range is from 60 to 600 seconds. The default is 300.

Command Default

No limit

Command Modes

Router configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **redistribute maximim-prefix** command to limit the number of routes redistributed into EIGRP. Use the **clear ip eigrp redistribute** command if all routes are withdrawn.

Examples

This example shows how to limit the number of redistributed routes into EIGRP:

```
switch# configure terminal
switch(config)# router eigrp 201
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# redistribute maximum-prefix 1000 75
switch(config-router-af)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
feature eigrp	Enables the EIGRP feature.
redistribute (EIGRP)	Configures route redistribution for EIGRP.
show running-config eigrp	Displays the EIGRP running configuration.

Review Draft -- Cisco Confidential

restart eigrp (EIGRP)

To restart an Enhanced Interior Gateway Routing Protocol (EIGRP) instance and remove all associated neighbors, use the **restart** command.

restart eigrp *instance-tag*

Syntax Description

instance-tag	Name for an EIGRP routing instance. The name can be a maximum of 20 alphanumeric characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to restart the OSPFv2 instance and remove all neighbors:

```
switch# configure terminal
switch(config)# restart eigrp Test1
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration in the startup configuration file.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

router eigrp

To configure a routing process and enter router configuration mode for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **router eigrp** command. To turn off the EIGRP routing process, use the **no** form of this command.

router eigrp *instance-tag*

no router eigrp *instance-tag*

Syntax Description

instance-tag	Name of an EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure a routing process for EIGRP:

```
switch(config)# router eigrp 1
switch(config-router)#
```

Related Commands

Command	Description
default-information	Controls the distribution of a default route.
default-metric	Configures the default metric for routes redistributed into EIGRP.
distance	Configures the administrative distance.
maximum-paths	Configures the maximum number of equal-cost paths.
redistribute	Configures route redistribution for EIGRP.
router-id	Configures the router ID.
timers	Configures the EIGRP timers.

Review Draft -- Cisco Confidential

router-id (EIGRP)

To configure a router ID for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **router-id** command. To cause the software to use the default method of determining the router ID, use the **no** form of this command.

router-id *router-id*

no router-id

Syntax Description

router-id	32-bit router ID value specified in four-part, dotted-decimal notation.

Command Default

If this command is not configured, EIGRP chooses an IPv4 address as the router ID from one of its interfaces.

Command Modes

Address family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **router-id** command to manually specify a unique 32-bit numeric value for the router ID. This action ensures that EIGRP can function regardless of the interface address configuration.

This command requires the LAN Base Services license.

Examples

This example shows how to assign the IP address of 192.0.2.1 to the EIGRP process 1:

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4
switch(config-router-af)# router-id 192.0.2.1
```

Related Commands

Command	Description
show ip eigrp	Displays a summary of the EIGRP processes.

Review Draft -- Cisco Confidential

S Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with S.

Review Draft -- Cisco Confidential

shutdown (EIGRP)

To shut down an instance of Enhanced Interior Gateway Routing Protocol (EIGRP), use the **shutdown** command. To disable this function, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Address family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **shutdown** command to disable an instance of EIGRP without removing the configuration.

This command requires the LAN Base Services license.

Examples

This example shows how to disable eigrp 209:

```
switch(config)# router eigrp 209
switch(config-router)# shutdown
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration in the startup configuration file.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

stub

To configure a router as a stub using the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **stub** command. To disable the EIGRP stub routing feature, use the **no** form of this command.

stub [**direct** | **leak-map** *map-name*| **receive-only** | **redistributed**]

no stub [**direct** | **leak-map** *map-name*| **receive-only** | **redistributed**]]

Syntax Description

direct	(Optional) Advertises directly connected routes.
leak-map *map-name*	(Optional) Allows dynamic prefixes based on the leak map.
receive-only	(Optional) Sets the router as a receive-only neighbor.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.

Command Default

Disabled

Command Modes

Address-family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **stub** command to configure a router as a stub where the router directs all IP traffic to a distribution router.

The **direct** keyword permits EIGRP stub routing to advertise connected routes. This option is enabled by default.

The **receive-only** keyword restricts the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword does not permit any other option to be specified because it prevents any type of route from being sent.

The **redistributed** keyword permits EIGRP stub routing to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP does not advertise redistributed routes.

If you use any of these four keywords (**direct**, **leak-map**, **receive-only**, **redistributed**) with the **stub** command, only the route types specified by the particular keyword(s) are advertised.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the router as a receive-only neighbor:

```
switch(config)# router eigrp 1
switch(config-router)# stub receive-only
```

Review Draft -- Cisco Confidential

```
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.
show ip eigrp neighbors	Displays EIGRP neighbor information.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) **show** commands.

Review Draft -- Cisco Confidential

show ip eigrp

To display a summary of the Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the **show ip eigrp** command.

show ip eigrp [*instance-tag*]

Syntax Description

instance-tag	(Optional) Name of the EIGRP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display all the EIGRP instances:

```
switch# show ip eigrp
IP-EIGRP AS 65535 ID 3.1.1.1 VRF default
  Process-tag: Test1
  Status: running
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Number of EIGRP interfaces: 8 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 8
  Redistributing:
    direct route-map SVI-EIGRP
  Graceful-Restart: Enabled
  Stub-Routing: Disabled
  NSF converge time limit/expiries: 120/0
  NSF route-hold time limit/expiries: 240/0
  NSF signal time limit/expiries: 20/0
  Redistributed max-prefix: Disabled
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
router eigrp	Configures an EIGRP instance.
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show ip eigrp accounting

To display prefix accounting information for the Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the **show ip eigrp accounting** command.

show ip eigrp [*instance-tag*] **accounting** [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) Name of the EIGRP instance. This option is available when a virtual routing and forwarding (VRF) instance is not specified. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display the EIGRP accounting information:

```
switch# show ip eigrp accounting
IP-EIGRP Accounting Statistics for AS 65535 VRF default
Total Prefix Count: 3536

States: A-Adjacency, P-Pending, D-Down

State Address/Source   Interface        Prefix   Restart  Restart/
                                        Count     Count   Reset(s)
 A    Redistributed    ----              118        0        0
 A    10.20.150.2      Po2001            3413       0        0
 A    10.20.200.2      Po2000            3418       0        0
 A    10.0.1.1         Eth1/26           3419       0        0
 A    10.50.2.1        Eth2/5            3419       0        0
 A    10.50.1.1        Eth2/6            3419       0        0
 A    10.50.3.1        Eth2/7            3419       0        0
 A    10.20.5.2        Eth3/11           3419       0        0
```

Review Draft -- Cisco Confidential

```
 A    10.20.6.2         Eth3/12           3419       0         0
switch#
```

Related Commands

Command	Description
router eigrp	Configures an EIGRP instance.
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show ip eigrp interfaces

To display information about interfaces configured for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ip eigrp interfaces** command.

show ip eigrp [*instance-tag*] **interfaces** [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}] [**brief**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) EIGRP Instance. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	(Optional) Specifies the VLAN interface. The range is from 1 to 4094.
brief	(Optional) Displays a brief summary of EIGRP interface information.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

This command shows all interfaces for the default VRF if no VRF or no interface is specified.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip eigrp interfaces** command to determine on which interfaces EIGRP is active and learn information about EIGRP related to those interfaces.

If you specify an interface, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If you specify an autonomous system, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

This command requires the LAN Base Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to display information about EIGRP interfaces:

```
switch# show ip eigrp interfaces brief
IP-EIGRP interfaces for process 65535 VRF default

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Eth1/26            1        0/0       16       0/1          64           0
Eth2/5             1        0/0       16       0/1          64           0
Eth2/6             1        0/0       16       0/1          64           0
Eth2/7             1        0/0       13       0/1          50           0
Eth3/11            1        0/0       18       0/1          80           0
Eth3/12            1        0/0       14       0/1          64           0
Po2000             1        0/0       13       0/1          72           0
Po2001             1        0/0       20       0/1          128          0
switch#
```

This example shows how to display information about a particular EIGRP interface:

```
switch# show ip eigrp interfaces ethernet 2/5
IP-EIGRP interfaces for process 65535 VRF default

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Eth2/5             1        0/0       16       0/1          64           0
  Hello interval is 5 sec
  Holdtime interval is 15 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/178  Un/reliable ucasts: 292/17
  Mcast exceptions: 4  CR packets: 4  ACKs suppressed: 8
  Retransmissions sent: 8  Out-of-sequence rcvd: 146
  Authentication mode is not set
switch#
```

Related Commands

Command	Description
show ip eigrp neighbors	Displays the neighbors discovered by EIGRP.
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show ip eigrp neighbors

To display information about neighbors discovered by the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ip eigrp neighbors** command.

show ip eigrp [*instance-tag*] **neighbors** [**detail**] [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
detail	(Optional) Displays detailed EIGRP neighbor information.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	(Optional) Specifies the VLAN interface. The range is from 1 to 4094.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

This command displays all neighbors for the default VRF on all interfaces if no VRF or interface is specified.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip eigrp neighbors** command to determine when neighbors become active and inactive. This command is also useful for debugging certain types of transport problems.

This command requires the LAN Base Services license.

Examples

This example shows how to display information about EIGRP neighbors:

Review Draft -- Cisco Confidential

```
switch# show ip eigrp neighbors
IP-EIGRP neighbors for process 65535 VRF default
H   Address                 Interface       Hold  Uptime   SRTT   RTO  Q  Seq
                                            (sec)          (ms)       Cnt Num
7   10.20.150.2             Po2001          12    03:44:02  20   200   0   10331
6   10.20.200.2             Po2000          14    03:44:02  13   200   0   158157
5   10.40.1.1               Eth1/26         13    03:44:14  16   200   0   158164
4   10.50.2.1               Eth2/5          12    03:44:14  16   200   0   158166
3   10.50.1.1               Eth2/6          13    03:44:15  16   200   0   158165
2   10.50.3.1               Eth2/7          11    03:44:15  13   200   0   158167
1   10.20.5.2               Eth3/11         14    03:44:16  18   200   0   158158
0   10.20.6.2               Eth3/12         11    03:44:17  14   200   0   158163
switch#
```

This example shows how to display detailed information about EIGRP neighbors:

```
switch# show ip eigrp neighbors detail
IP-EIGRP neighbors for process 65535 VRF default
H   Address                 Interface       Hold  Uptime   SRTT   RTO  Q  Seq
                                            (sec)          (ms)       Cnt Num
7   10.20.150.2             Po2001          10    03:45:21  20   200   0   10331
   Version 12.4/1.2, Retrans: 4, Retries: 0, Prefixes: 3413
6   10.20.200.2             Po2000          12    03:45:22  13   200   0   158157
   Version 12.4/1.2, Retrans: 2, Retries: 0, Prefixes: 3418
5   10.40.1.1                Eth1/26         11    03:45:34  16   200   0   158164
   Version 12.4/1.2, Retrans: 5, Retries: 0, Prefixes: 3419
4   10.50.2.1               Eth2/5          12    03:45:34  16   200   0   158166
   Version 12.4/1.2, Retrans: 8, Retries: 0, Prefixes: 3419
3   10.50.1.1               Eth2/6          12    03:45:35  16   200   0   158165
   Version 12.4/1.2, Retrans: 4, Retries: 0, Prefixes: 3419
2   10.50.3.1               Eth2/7          13    03:45:35  13   200   0   158167
   Version 12.4/1.2, Retrans: 3, Retries: 0, Prefixes: 3419
1   10.20.5.2               Eth3/11         12    03:45:36  18   200   0   158158
   Version 12.4/1.2, Retrans: 7, Retries: 0, Prefixes: 3419
0   10.20.6.2               Eth3/12         10    03:45:36  14   200   0   158163
   Version 12.4/1.2, Retrans: 5, Retries: 0, Prefixes: 3419
switch#
```

Related Commands

Command	Description
clear ip eigrp neighbors	Clears neighbors for EIGRP.
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show ip eigrp route

To display the Enhanced Interior Gateway Routing Protocol (EIGRP) routes, use the **show ip eigrp route-map statistics** command in any mode.

show ip eigrp [*instance-tag*] **route** [*ip-prefix/length*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
ip-prefix/length	(Optional) IP address in four-part, dotted-decimal notation with a network mask indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are 1s, and the corresponding bits of the address are the network address.
active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all entries in the EIGRP topology table.
detail-links	(Optional) Displays detailed information for all entries in the EIGRP topology table.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of theEIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Command History

Usage Guidelines

This command requires a LAN Base Services license.

Examples

This example shows how to display the EIGRP routes:

```
switch# show ip eigrp route
```

Review Draft -- Cisco Confidential

```
IP-EIGRP Topology Table for AS(65535)/ID(3.1.1.1) VRF default

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.0.2.0/24, 7 successors, FD is 13056
        via 192.0.2.1 (13056/12800), Ethernet2/7
        via 192.0.2.5 (13056/12800), Ethernet1/26
        via 192.0.2.3 (13056/12800), Ethernet3/12
        via 192.0.2.6 (13056/12800), Ethernet3/11
        via 192.0.2.4 (13056/12800), port-channel2000
        via 192.0.2.2 (13056/12800), Ethernet2/6
        via 192.0.2.7 (13056/12800), Ethernet2/5
P 192.0.2.1/24, 7 successors, FD is 13056
        via 192.0.2.1 (13056/12800), Ethernet2/7
        via 192.0.2.2 (13056/12800), Ethernet2/6
        via 192.0.2.3 (13056/12800), Ethernet3/12
        via 192.0.2.4 (13056/12800), port-channel2000
        via 192.0.2.6 (13056/12800), Ethernet3/11
        via 192.0.2.5 (13056/12800), Ethernet1/26
        via 192.0.2.7 (13056/12800), Ethernet2/5
P 192.0.2.5/24, 7 successors, FD is 13056
        via 192.0.2.1 (13056/12800), Ethernet2/7
<--Output truncated-->
switch#
```

Related Commands

Command	Description
clear ip eigrp route-map statistics	Clears route-map statistics for EIGRP.
show ip eigrp traffic	Displays EIGRP traffic statistics.
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show ip eigrp route-map statistics

To display the route redistribution statistics for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ip eigrp route-map statistics** command in any mode.

show ip eigrp [*instance-tag*] **route-map statistics redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
bgp	Displays policy statistics for the Border Gateway Protocol (BGP).
direct	Displays policy statistics for directly connected routes only.
eigrp	Displays policy statistics for EIGRP.
ospf	Displays policy statistics for the Open Shortest Path First (OSPF) protocol.
rip	Displays policy statistics for the Routing Information Protocol (RIP).
static	Displays policy statistics for IP static routes.
id	For the **bgp** keyword, an autonomous system number. The range for 2-byte numbers is from 1 to 65535. The range for 4-byte numbers is from 1.0 to 65535.65535. For the **eigrp** keyword, an EIGRP instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string. For the **ospf** keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires a LAN Base Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to display route-map statistics for EIGRP:

```
switch# show ip eigrp route-map statistics redistribute direct
C: No. of comparisions, M: No. of matches

route-map SVI-EIGRP permit 10
  match source-protocol direct                                C: 129    M: 0
Total accept count for policy: 129
Total reject count for policy: 0
switch#
```

Related Commands

Command	Description
clear ip eigrp route-map statistics	Clears route-map statistics for EIGRP.
show ip eigrp traffic	Displays EIGRP traffic statistics.
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show ip eigrp topology

To display the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show ip eigrp topology** command.

show ip eigrp [*instance-tag*] **topology** [*ip-address/length*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
ip-address/length	(Optional) IP address in four-part, dotted-decimal notation with a network mask indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are 1s, and the corresponding bits of the address are the network address.
active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all entries in the EIGRP topology table.
detail-links	(Optional) Displays detailed information for all entries in the EIGRP topology table.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

This command displays information for the default VRF if no VRF is specified.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip eigrp topology** command to determine Diffusing Update Algorithm (DUAL) states and to debug possible DUAL problems.

When you use the **show ip eigrp topology** command without any keywords or arguments, Cisco Nexus 6000 displays only routes that are feasible successors.

Review Draft -- Cisco Confidential

This command requires the LAN Base Services license.

Examples

This example shows how to display the EIGRP topology table. The EIGRP metrics for specified internal routes and external routes are displayed.

```
switch# show ip eigrp topology 192.0.2.0/24
IP-EIGRP (AS 65535): Topology entry for 192.0.2.0/24
  State is Passive, Query origin flag is 1, 7 Successor(s), FD is 13056
  Routing Descriptor Blocks:
  192.0.2.1 (Ethernet2/7), from 192.0.2.1, Send flag is 0x0
      Composite metric is (13056/12800), Route is External
      Vector metric:
        Minimum bandwidth is 500000 Kbit
        Total delay is 310 microseconds
        Reliability is 200/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 1.1.1.1
        AS number of route is 0
        External protocol is OSPF, external metric is 0
        Administrator tag is 0 (0x00000000)
  192.0.2.2 (Ethernet2/6), from 192.0.2.2, Send flag is 0x0
      Composite metric is (13056/12800), Route is External
      Vector metric:
        Minimum bandwidth is 500000 Kbit
        Total delay is 310 microseconds
        Reliability is 200/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 1.1.1.1
        AS number of route is 0
        External protocol is OSPF, external metric is 40
        Administrator tag is 0 (0x00000000)
  192.0.2.3 (Ethernet3/12), from 192.0.2.3, Send flag is 0x0
      Composite metric is (13056/12800), Route is External
      Vector metric:
        Minimum bandwidth is 500000 Kbit
        Total delay is 310 microseconds
        Reliability is 200/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 1.1.1.1
        AS number of route is 0
        External protocol is OSPF, external metric is 40
        Administrator tag is 0 (0x00000000)
  192.0.2.6 (Ethernet3/11), from 192.0.2.6, Send flag is 0x0
      Composite metric is (13056/12800), Route is External
      Vector metric:
        Minimum bandwidth is 500000 Kbit
        Total delay is 310 microseconds
        Reliability is 200/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 1.1.1.1
```

Review Draft -- Cisco Confidential

```
      AS number of route is 0
      External protocol is OSPF, external metric is 40
      Administrator tag is 0 (0x00000000)
  192.0.2.4 (port-channel2000), from 192.0.2.4, Send flag is 0x0
    Composite metric is (13056/12800), Route is External
    Vector metric:
      Minimum bandwidth is 500000 Kbit
      Total delay is 310 microseconds
      Reliability is 200/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
    External data:
      Originating router is 1.1.1.1
      AS number of route is 0
      External protocol is OSPF, external metric is 40
      Administrator tag is 0 (0x00000000)
  192.0.2.2 (Ethernet2/6), from 192.0.2.2, Send flag is 0x0
    Composite metric is (13056/12800), Route is External
    Vector metric:
      Minimum bandwidth is 500000 Kbit
      Total delay is 310 microseconds
      Reliability is 200/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
    External data:
      Originating router is 1.1.1.1
      AS number of route is 0
      External protocol is OSPF, external metric is 40
      Administrator tag is 0 (0x00000000)
  192.0.2.7 (Ethernet2/5), from 192.0.2.7, Send flag is 0x0
    Composite metric is (13056/12800), Route is External
    Vector metric:
      Minimum bandwidth is 500000 Kbit
      Total delay is 310 microseconds
      Reliability is 200/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
    External data:
      Originating router is 1.1.1.1
      AS number of route is 0
      External protocol is OSPF, external metric is 40
      Administrator tag is 0 (0x00000000)
  192.0.2.200 (port-channel2001), from 192.0.2.200, Send flag is 0x0
    Composite metric is (13312/13056), Route is External
    Vector metric:
      Minimum bandwidth is 500000 Kbit
      Total delay is 320 microseconds
      Reliability is 200/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 2
    External data:
      Originating router is 1.1.1.1
      AS number of route is 0
      External protocol is OSPF, external metric is 40
      Administrator tag is 0 (0x00000000)
switch#
```

This example show how to display all the entries in the EIGRP topology table:

```
switch(config)# show ip eigrp topology all-links
```

Review Draft -- Cisco Confidential

This example shows how to display the detailed information for all entries in the EIGRP topology table:

```
switch(config)# show ip eigrp topology detail-links
```

This example shows how to display a summary of the topology table:

```
switch(config)# show ip eigrp topology summary
IP-EIGRP Topology Table for AS(65535)/ID(3.1.1.1) VRF default

Head serial 3, next serial 15631
3536 routes, 0 pending replies, 0 dummies
IP-EIGRP(0) enabled on 8 interfaces, 8 neighbors present on 8 interfaces
Quiescent interfaces:  Eth3/11 Po2000 Po2001 Eth2/7 Eth2/5 Eth2/6 Eth1/26 Eth3/12
switch#
```

This example shows how to display the active entries in the topology table:

```
switch(config-if)# show ip eigrp topology active
```

This example shows how to display zero-successors in the topology table:

```
switch(config-router)# show ip eigrp topology zero-successors
```

This example shows how to display pending entries:

```
switch(config)# show ip eigrp topology pending
```

Related Commands

Command	Description
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show ip eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets sent and received, use the **show ip eigrp traffic** command.

show ip eigrp [*instance-tag*] **traffic** [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

This command displays information for the default VRF if no VRF is specified.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip eigrp traffic** command to find the number of packets sent and received by this EIGRP instance.

In addition, this command is useful in determining whether packets from one node are not reaching the neighboring node due to connectivity or configuration problems.

This command requires the LAN Base Services license.

Examples

This example shows how to display the EIGRP traffic statistics:

```
switch# show ip eigrp traffic
IP-EIGRP Traffic Statistics for AS 65535 VRF default
  Hellos sent/received: 29838/44756
  Updates sent/received: 1448/1775
  Queries sent/received: 33/47
  Replies sent/received: 31/31
  Acks sent/received: 1759/2061
  Input queue high water mark 33, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: (no process)
  PDM Process ID: (no process)
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show running-config eigrp	Displays EIGRP running configuration information.

Review Draft -- Cisco Confidential

show running-config eigrp

To display the running configuration for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 networks, use the **show running-config eigrp** command.

show running-config eigrp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

Need new output

This example shows how to display the running configuration for EIGRP:

```
switch# show running-config eigrp

!Command: show running-config eigrp
!Time: Mon Feb 28 05:47:18 2011

version 5.0(3)N1(1)
feature eigrp

router eigrp Test1
  autonomous-system 65535
  default-metric 500000 30 200 1 1500
  redistribute direct route-map SVI-EIGRP

interface port-channel2000
  ip router eigrp Test1

interface port-channel2001
  ip router eigrp Test1

interface Ethernet1/26
  ip router eigrp Test1

interface Ethernet2/5
  ip router eigrp Test1
```

Review Draft -- Cisco Confidential

```
interface Ethernet2/6
  ip router eigrp Test1

interface Ethernet2/7
  ip router eigrp Test1

interface Ethernet3/11
  ip router eigrp Test1

interface Ethernet3/12
  ip router eigrp Test1


switch#
```

Related Commands

Command	Description
router ospf	Creates an OSPF instance.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

T Commands

This chapter describes the Cisco NX-OS Enhanced Interior Gateway Routing Protocol (EIGRP) commands that begin with T.

Review Draft -- Cisco Confidential

timers active-time

To adjust the Enhanced Interior Gateway Routing Protocol (EIGRP) time limit for the active state, use the **timers active-time** command. To disable this function, use the **no** form of the command.

timers active-time [*time-limit* | **disabled**]

no timers active-time

Syntax Description

time-limit	(Optional) Active time limit (in minutes). The range is from 1 to 65535 minutes. The default value is 3.
disabled	(Optional) Disables the timers and permits the routing wait time to remain active indefinitely.

Command Default

Disabled

Command Modes

Address family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers active-time** command to control the time that the router waits (after a query is sent) before declaring the route to be in the stuck in active (SIA) state.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an indefinite routing wait time on the specified EIGRP route:

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers active-time disabled
switch(config-router-af)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

timers nsf converge

To adjust the time limit for nonstop forwarding (NSF) convergence for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **timers nsf converge** command. To disable this function, use the **no** form of the command.

timers nsf converge *seconds*

no timers nsf converge

Syntax Description

seconds	Time limit for convergence after an NSF switchover (in seconds). The range is from 60 to 180 seconds. The default value is 120.

Command Default

120 seconds

Command Modes

Address family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers nsf converge** command to control the time that the router waits for convergence after a switchover.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the NSF convergence time for EIGRP:

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf converge 100
switch(config-router-af)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

timers nsf route-hold

To set the timer that determines how long an NSF-aware Enhanced Interior Gateway Routing Protocol (EIGRP) router holds routes for an inactive peer, use the **timers nsf route-hold** command. To return the route hold timer to the default value, use the **no** form of this command.

timers nsf route-hold *seconds*

no timers nsf route-hold

Syntax Description

seconds	Time, in seconds, that EIGRP holds routes for an inactive peer. The range is from 20 to 300 seconds. The default is 240.

Command Default

EIGRP NSF awareness is enabled.
seconds: 240

Command Modes

Address family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers nsf route-hold** command to set the maximum period of time that the NSF-aware router holds known routes for an NSF-capable neighbor during a switchover operation or a well-known failure condition. The route hold timer is configurable so that you can tune network performance and avoid undesired effects, such as "black holing" routes (advertising invalid routes) if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

This command requires the LAN Base Services license.

Examples

This example shows how to set the route hold timer value for an NSF-aware router to 2 minutes (120 seconds):

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf route-hold 120
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

Review Draft -- Cisco Confidential

timers nsf signal

To set the time limit to signal a nonstop forwarding (NSF) restart for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **timers nsf signal** command. To return the route hold timer to the default, use the **no** form of this command.

timers nsf signal *seconds*

no timers nsf signal

Syntax Description

seconds	Time, in seconds, that EIGRP waits for a peer to signal an NSF restart. The range is from 10 to 360 seconds.

Command Default

EIGRP NSF awareness is enabled

Command Modes

Address family configuration mode
Router configuration mode
Router VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers nsf signal** command to set the maximum period of time that the NSF-aware router waits for an NSF-capable neighbor to signal a restart.

This command requires the LAN Base Services license.

Examples

This example shows how to set the signal timer value for an NSF-aware router to the maximum (30 seconds):

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf signal 30
switch(config-router-af)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip eigrp	Displays EIGRP information.

<I_Italic>Review Draft -- Cisco Confidential

PART 3

HSRP Commands

Review Draft -- Cisco Confidential

A Commands

This chapter describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) commands that begin with A.

Review Draft -- Cisco Confidential

authentication (HSRP)

To configure authentication for the Hot Standby Router Protocol (HSRP), use the **authentication** command. To disable authentication, use the **no** form of this command.

authentication {*string* | **md5** {**key-chain** *key-chain* | **key-string** {**0** | **7**} *text* [**timeout** *seconds*]} | **text** *string*}

no authentication {*string* | **md5** {**key-chain** *key-chain* | **key-string** {**0** | **7**} *text* [**timeout** *seconds*]} | **text** *string*}

Syntax Description

md5	Specifies the Message Digest 5 (MD5) authentication.
key-chain *key-chain*	Identifies a group of authentication keys.
key-string	Specifies the secret key for MD5 authentication.
0	Specifies a clear text string.
7	Specifies an encrypted string.
text	Secret key for MD5 authentication. The range is from 1 to 255 characters. We recommend that you use at least 16 characters.
timeout *seconds*	(Optional) Specifies the authentication timeout value. The range is from 0 to 32767.
text *string*	Specifies an authentication string. The range is from 1 to 255 characters. The default string is “cisco”.

Command Default

Disabled

Command Modes

HSRP configuration or HSRP template mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **authentication text** command to prevent misconfigured routers from participating in HSRP groups that they are not intended to participate in. The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers in the same group to ensure interoperation. HSRP protocol packets that do not authenticate are ignored.

Caution If you configure two routers with identical HSRP IP addresses but with different authentication strings, then neither router is aware of the duplication.

Examples

This example shows how to configure an authentication string for HSRP group 2:

```
switch# configure terminal
```

Review Draft -- Cisco Confidential

```
switch(config)# interface ethernet 0/1
switch(config-if)# no switchport
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 2
switch(config-if-hsrp)# priority 110
switch(config-if-hsrp)# preempt
switch(config-if-hsrp)# authentication text sanjose
switch(config-if-hsrp)# ip 10.0.0.3
switch(config-if-hsrp)# end
switch(config-if-hsrp)#
```

Related Commands

Command	Description
feature hsrp	Enables HSRP and enters HSRP configuration mode.
hsrp group	Creates an HSRP group.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

D Commands

This chapter describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) commands that begin with D.

Review Draft -- Cisco Confidential

delay minimum

To delay the Hot Standby Router Protocol (HSRP) initialization after a reload or after an interface comes up, use the **delay minimum** command. To disable this function, use the **no** form of this command.

delay minimum [*min-delay*] **reload** [*reload-delay*]

no delay minimum [*min-delay*] **reload** [*reload-delay*]

Syntax Description

min-delay	(Optional) Minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This period applies to all subsequent interface events. The default is 0 seconds.
reload *reload-delay*	Specifies the time period to delay HSRP group initialization after the router has reloaded. This period applies only to the first interface-up event after the router has reloaded. The default is 0 seconds.

Command Default

The HSRP delay default is 0 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **delay hsrp** command to delay HSRP initialization either after a reload or after an interface comes up. This configuration allows the interface and router to stabilize after the interface comes up and helps to prevent HSRP state flapping.

Examples

This example shows how to configure a minimum delay of 3 seconds and a group initialization delay of 10 seconds:

```
switch(config)# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 172.16.6.5 255.255.255.0
switch(config-if)# hsrp 1
switch(config-if-hsrp)# delay minimum 3 reload 10
switch(config-if-hsrp)# ip 172.16.6.100
```

Related Commands

Command	Description
feature hsrp	Enables the HSRP configuration.

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) commands that begin with F.

Review Draft -- Cisco Confidential

feature hsrp

To enter Hot Standby Router Protocol (HSRP) configuration mode and enable HSRP, use the **feature hsrp** command. To disable HSRP, use the **no** form of this command.

feature hsrp

no feature hsrp

Syntax Description

The command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the HSRP feature before you can configure HSRP.

This command does not require a license.

Examples

This example shows how to enable HSRP on the switch:

```
switch# configure terminal
switch(config)# feature hsrp
switch(config)#
```

This example shows how to disable HSRP:

```
switch# configure terminal
switch(config)# no feature hsrp
switch(config)#
```

Related Commands

Command	Description
hsrp group	Creates and activates an HSRP group.
show feature	Displays the status of features on a switch.
show hsrp	Displays HSRP information.

Review Draft -- Cisco Confidential

H Commands

This chapter describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) commands that begin with H.

Review Draft -- Cisco Confidential

hsrp

To enter Hot Standby Router Protocol (HSRP) configuration mode and create an HSRP group, use the **hsrp** command. To disable HSRP, use the **no** form of this command.

hsrp *group-number* **ipv4**

no hsrp *group-number* **ipv4**

Syntax Description

group-number	Number of HSRP groups that can be configured on a Gigabit Ethernet port, including the main interfaces and subinterfaces. The range is from 1 to 255. The default value is 0.
ipv4	(Optional) Sets the HSRP group for IPv4.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must globally enable HSRP before you can configure any HSRP options or create an HSRP group.

Examples

This example shows how to create and activate an HSRP group:

```
switch# configure terminal
switch(config)# interface ethernet 0
switch(config-if)# no switchport
switch(config-if)# ip address 172.16.6.5 255.255.255.0
switch(config-if)# hsrp 1
switch(config-if-hsrp)#
```

This example shows how to create and activate an HSRP group for IPv6:

```
switch# configure terminal
switch(config)# interface ethernet 1
switch(config-if)# no switchport
switch(config-if)# ipv6 address 172.16.6.5 255.255.255.0
switch(config-if)# hsrp 1
switch(config-if-hsrp)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
feature hsrp	Enables HSRP configuration.
ip address	Creates a virtual IP address for the HSRP group. The IP address must be in the same subnet as the interface IP address.
show hsrp	Displays HSRP information.

Review Draft -- Cisco Confidential

hsrp delay

To delay Hot Standbu Router Protocol (HSRP) initialization after a reload or after an interface comes up, use the **hsrp delay** command. To disable this function, use the **no** form of this command.

hsrp delay {**minimum** *min-delay* | **reload** *reload-delay*}

no delay {**minimum** *min-delay* | **reload** *reload-delay*}

Syntax Description

minimum *min-delay*	Specifies the minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This period applies to all subsequent interface events. The range is from 1 to 10,000. The default is 0 seconds.
reload *reload-delay*	Specifies the time period to delay HSRP group initialization after the router has reloaded. This period applies only to the first interface-up event after the router has reloaded. The range is from 1 to 10,000. The default is 0 seconds.

Command Default

The HSRP delay default is 0 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **hsrp delay** command to delay HSRP initialization either after a reload or after an interface comes up. This configuration allows the interface and router to stabilize after the interface comes up and helps prevent HSRP state flapping.

Examples

This example shows how to configure a minimum delay of 3 seconds and a group initialization delay of 10 seconds:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 172.16.6.5 255.255.255.0
switch(config-if)# hsrp 1
switch(config-if-hsrp)# hsrp delay minimum 3 reload 10
switch(config-if-hsrp)#
```

Related Commands

Command	Description
feature hsrp	Enables the HSRP configuration.

Review Draft -- Cisco Confidential

Command	Description
hsrp	Creates HSRP groups.
show hsrp delay	Displays the HSRP delay information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) commands that begin with I.

Review Draft -- Cisco Confidential

ip (HSRP)

To assign a virtual address to an HSRP group, use the **ip** command. To disable HSRP in the group, use the **no** form of this command.

ip [**autoconfig** | *ip-address* [**secondary**]]

no ip [**autoconfig** | *ip-address* [**secondary**]]

Syntax Description

autoconfig	(Optional) Generates a link-local address from the link-local prefix and a modified EUI-64 format Interface Identifier, where the EUI-64 Interface Identifier is created from the relevant HSRP virtual MAC address.
ip-address	(Optional) Virtual IP address for the virtual router (HSRP group). The IP address must be in the same subnet as the interface IP address. You must configure the virtual IP address for at least one of the routers in the HSRP group. Other routers in the group will pick up this address. The IP address can be an IPv4 address.
secondary	(Optional) Indicates that the IPv4 address is a secondary HSRP virtual address.

Command Default

Disabled

Command Modes

HSRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip** command to activate HSRP on the configured interface. If you configure a virtual IP address, that address is the designated virtual IP address for the entire HSRP group. For IPv4 groups, if you do not configure a virtual IP address, the gateway learns the virtual IP address from another gateway in the same HSRP group. To allow HSRP to elect an active virtual gateway (AVG), you must configure at least one gateway on the LAN with a virtual IP address.

Configuring the virtual IP address on the AVG always overrides a virtual IP address that is in use.

When you configure the **ip** command for an IPv4 HSRP group on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to map an IP address to a MAC address. The HSRP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the HSRP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Review Draft -- Cisco Confidential

Note You must configure all HSRP options before you use the **ip** command to assign a virtual IP address and activate the HSRP group so that you can avoid authentication error messages and unexpected state changes that can occur in other routers when a group is enabled first and then there is a delay before the configuration is created. We recommend that you always specify an IP address.

Examples

This example shows how to activate HSRP for group 10 on Ethernet interface 1/1. The virtual IP address used by the HSRP group is set to 192.0.2.10.

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.32 255.255.255.0
switch(config-if)# hsrp 10
switch(config-if-hsrp)# ip 192.0.2.10
```

This example shows how to activate HSRP for group 10 on Ethernet interface 2/1. The virtual IP address used by the HSRP group will be learned from another gateway configured to be in the same HSRP group.

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# hsrp 10
switch(config-if-hsrp)#
```

This example shows how to activate HSRP for group 2 on Ethernet interface 1/1 and creates a secondary IP address on the interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no switchport
switch(config-if)# ip address 20.20.20.1 255.255.255.0 secondary
switch(config-if)# ip address 10.10.10.1 255.255.255.0
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 10.10.10.2
switch(config-if-hsrp)# ip 20.20.20.2 secondary
```

Related Commands

Command	Description
feature hsrp	Enables the HSRP configuration.
show hsrp	Displays HSRP information.

Review Draft -- Cisco Confidential

ipv6 (HSRP)

To assign a virtual address to an HSRP group, use the **ip** command. To disable HSRP in the group, use the **no** form of this command.

ipv6 [**autoconfig** | *ip-address* [**secondary**]]

no ipv6 [**autoconfig** | *ip-address* [**secondary**]]

Syntax Description

autoconfig	(Optional) Generates a link-local address from the link-local prefix and a modified EUI-64 format Interface Identifier, where the EUI-64 Interface Identifier is created from the relevant HSRP virtual MAC address.
ipv6-address	(Optional) Virtual IPv6 address for the virtual router (HSRP group). The IPv6 address must be in the same subnet as the interface IPv6 address. You must configure the virtual IPv6 address for at least one of the routers in the HSRP group. Other routers in the group will pick up this address.
secondary	(Optional) Indicates that the IPv6 address is a secondary HSRP virtual address.

Command Default

Disabled

Command Modes

HSRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ipv6** command to activate HSRP on the configured interface. If you configure a virtual IPv6 address, that address is the designated virtual IPv6 address for the entire HSRP group. For IPv6 groups, if you do not configure a virtual IPv6 address, the gateway learns the virtual IPv6 address from another gateway in the same HSRP group. To allow HSRP to elect an active virtual gateway (AVG), you must configure at least one gateway on the LAN with a virtual IPv6 address.

Configuring the virtual IPv6 address on the AVG always overrides a virtual IPv6 address that is in use.

When you configure the **ipv6** command for an IPv6 HSRP group on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to map an IPv6 address to a MAC address. The HSRP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the HSRP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Note You must configure all HSRP options before you use the **ipv6** command to assign a virtual IPv6 address and activate the HSRP group so that you can avoid authentication error messages and unexpected state changes that can occur in other routers when a group is enabled first and then there is a delay before the configuration is created. We recommend that you always specify an IPv6 address.

Review Draft -- Cisco Confidential

Examples

This example shows how to activate HSRP for group 10 on Ethernet interface 1/1. The virtual IPv6 address used by the HSRP group is set to 192.0.2.10.

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no switchport
switch(config-if)# ipv6 address 192.0.2.32 255.255.255.0
switch(config-if)# hsrp 10
switch(config-if-hsrp)# ipv6 192.0.2.10
```

This example shows how to activate HSRP for group 10 on Ethernet interface 2/1. The virtual IPv6 address used by the HSRP group will be learned from another gateway configured to be in the same HSRP group.

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# hsrp 10
switch(config-if-hsrp)#
```

This example shows how to activate HSRP for group 2 on Ethernet interface 1/1 and creates a secondary IPv6 address on the interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no switchport
switch(config-if)# ipv6 address 20.20.20.1 255.255.255.0 secondary
switch(config-if)# ipv6 address 10.10.10.1 255.255.255.0
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ipv6 10.10.10.2
switch(config-if-hsrp)# ipv6 20.20.20.2 secondary
```

Related Commands

Command	Description
feature hsrp	Enables the HSRP configuration.
show hsrp	Displays HSRP information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

P Commands

This chapter describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) commands that begin with P.

Review Draft -- Cisco Confidential

preempt (HSRP)

To configure a preemption delay, use the **preempt** command. To disable this feature, use the **no** form of this command.

preempt [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync** *sync-delay*}]

no preempt [**delay** {**minimum** *min-delay* | **reload** *rel-delay* | **sync** *sync-delay*}]

Syntax Description

delay minimum *min-delay*	(Optional) Specifies the minimum number of seconds that preemption is delayed to allow routing tables to be updated before a router becomes active. The default value is 0.
reload *rel-delay*	(Optional) Specifies the time delay after the router has reloaded. This period applies only to the first interface-up event after the router has reloaded. The default value is 0.
sync *sync-delay*	(Optional) Specifies the maximum number of seconds to allow IP redundancy clients to prevent preemption. When this period expires, preemption occurs regardless of the state of the IP redundancy clients. The default value is 0.

Command Default

The default delay time for all options is 0 seconds.

Command Modes

Interface configuration or HSRP template mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Specifying a minimum delay allows routing tables to be updated before a router becomes active. When a router first comes up, it does not have a complete routing table. A high-priority router will only delay preemption if it first receives a hello packet from a low-priority active router. If the high-priority router does not receive a hello packet from the low-priority active router when it is starting up, it assumes there is no active router for the group and becomes active as soon as possible.

Examples

This example shows how to configure a delay when a router becomes active when its priority is 110:

```
switch# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if)# no switchport
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 4
switch(config-if-hsrp)# priority 110
switch(config-if-hsrp)# preempt
switch(config-if-hsrp)# authentication text sanjose
switch(config-if-hsrp)# ip 10.0.0.3
switch(config-if-hsrp)# end
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
feature hsrp	Enables the HSRP configuration.
show hsrp	Displays HSRP information.

Review Draft -- Cisco Confidential

priority (HSRP)

To set the priority level within a Hot Standby Router Protocol (HSRP) group, use the **priority** command. To remove the priority level, use the **no** form of this command.

priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

no priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

Syntax Description

level	Interface priority for a virtual router. The range of values is from 1 to 255. If this router is the owner of the IP addresses, then the value is automatically set to 255. The default is 100.
forwarding-threshold	(Optional) Sets the threshold used by a virtual port channel (vPC) to determine when to fail over to the vPC trunk.
lower *lower-value*	(Optional) Sets the low threshold value. The range is from 1 to 255. The default is 1.
upper *upper-value*	(Optional) Sets the upper threshold value. The range is from 1 to 255. The default is 255.

Command Default

level: 100
lower-value: 1
upper-value: 255

Command Modes

HSRP configuration or HSRP template mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **priority** command to control which virtual router becomes the active router. HSRP compares the priorities of all virtual routers in the HSRP group and selects the router with the numerically highest priority. If two virtual routers have equal priority, HSRP selects the router with the highest IP address.

Examples

This example shows how to configure a virtual router with a priority of 254:

```
switch# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if)# no switchport
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 4
switch(config-if-hsrp)# priority 254
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
feature hsrp	Enables the HSRP configuration.
show hsrp	Displays HSRP information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS Hot Standby Router Protocol (HSRP) **show** commands.

Review Draft -- Cisco Confidential

show hsrp

To display Hot Standby Router Protocol (HSRP) information for each HSRP group, use the **show hsrp** command.

show hsrp [**interface** {**ethernet** *slot*/*port* | **port-channel** *number* | **vlan** *vlan-id*}] [**group** *group-number*] [**active** | **init** | **listen** | **standby**] [**all**] [**brief**] [**detail**] [**ipv4**]

Syntax Description

interface	(Optional) Specifies the interface for which to display HSRP information.
ethernet *slot*/*port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	Specifies the VLAN interface. The range is from 1 to 4094.
group *group-number*	(Optional) Specifies the HSRP group number of the interface to display information about. The range is from 0 to 4095.
active	(Optional) Displays HSRP groups that are in an active state.
init	(Optional) Displays HSRP groups that are in an initialization state.
listen	(Optional) Displays HSRP groups that are in an listen state.
standby	(Optional) Displays HSRP groups that are in an standby state.
all	(Optional) Displays all HSRP groups.
brief	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.
detail	(Optional) Displays detailed information about HSRP groups.
ipv4	(Optional) Displays HSRP IPv4 groups.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show hsrp** command to display information about HSRP groups. The **brief** keyword displays a single line of information about each virtual gateway or virtual forwarder.

If you have not configured authentication, the **show hsrp** command will display the following string:

```
Authentication text "cisco"
```

This is the default behavior of HSRP as defined in RFC 2281:

```
If no authentication data is configured, the RECOMMENDED default
value is 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00.
```

Review Draft -- Cisco Confidential

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to display the default information about HSRP:

```
switch# show hsrp
Vlan1 - Group 1 (HSRP-V1) (IPv4)
  Local state is Active, priority 150 (Cfged 150), may preempt
    Forwarding threshold(for vPC), lower: 1 upper: 150
  Preemption Delay (Seconds) Reload:300
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.793000 sec(s)
  Virtual IP address is 10.1.1.3 (Cfged)
  Active router is local
  Standby router is unknown
  Authentication text "cisco"
  Virtual mac address is 0000.0c07.ac01 (Default MAC)
  17 state changes, last state change 1w0d
  IP redundancy name is hsrp-Vlan1-1 (default)
...
```

Note The authentication text string in the preceding example indicates that authentication has not been configured on the interface.

This example shows how to display a brief summary of HSRP information:

```
switch# show hsrp brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active addr      Standby addr     Group addr
Vlan1       1   150  P Active   local            unknown          10.1.1.3        (conf)
Vlan2       2   150  P Active   local            unknown          10.1.2.3        (conf)
...
```

Related Commands

Command	Description
feature hsrp	Enables the HSRP feature.

Review Draft -- Cisco Confidential

show hsrp delay

To display the Hot Standby Router Protocol (HSRP) group delay information, use the **show hsrp delay** command.

show hsrp delay [**interface** {**ethernet** *slot/port* | **port-channel** *number*[**.***sub_if_number*] | **vlan** *vlan_id*}] [**group** *group-number*] [**all**] [**brief**]

Syntax Description

interface	(Optional) Specifies the interface type and number for which to display HSRP information.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface. The EtherChannel number is from 1 to 4096.
.*sub_if-number*	(Optional) Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	(Optional) Specifies the VLAN interface. The range is from 1 to 4094.
group *group-number*	(Optional) Specifies the HSRP group number of the interface to display information about. The range is from 0 to 4095.
all	(Optional) Specifies all HSRP information.
brief	(Optional) Specifies brief HSRP information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to display HSRP delay information:

```
switch# show hsrp delay
---------------------------------
Interface       Minimum    Reload
---------------------------------
Eth1/5          30         0
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
delay minimum	Configures the delay infromation for HSRP groups.
feature hsrp	Enables the HSRP feature.
hsrp delay	Configures the delay infromation for HSRP groups.

Review Draft -- Cisco Confidential

show hsrp summary

To display Hot Standby Router Protocol (HSRP) summary information for each HSRP group, use the **show hsrp summary** command.

show hsrp summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to display a summary of HSRP information:

```
switch# show hsrp summary

HSRP Summary:

Extended-hold (NSF) disabled
Global HSRP-BFD disabled

Total Groups: 1
     Version::    V1-IPV4: 1       V2-IPV4: 0      V2-IPV6: 0
       State::     Active: 0       Standby: 0       Listen: 0
       State::  V6-Active: 0    V6-Standby: 0    V6-Listen: 0

Total HSRP Enabled interfaces: 1

Total Packets:
             Tx - Pass: 0       Fail: 0
             Rx - Good: 0

Packet for unknown groups: 0

Total MTS: Rx: 25

switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
feature hsrp	Enables the HSRP feature.
hsrp	Configures HSRP groups.

Review Draft -- Cisco Confidential

<l_Italic>Review Draft -- Cisco Confidential

PART 5

Layer 3 Interfaces Commands

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS Layer 3 interfaces commands that begin with C.

Review Draft -- Cisco Confidential

clear ip arp

To clear the Address Resolution Protocol (ARP) information, use the **clear ip arp** command.

clear ip arp [*ip-addr* | **ethernet** *slot/port*[**.***sub_if*] | **loopback** *if_number* | **port-channel** *number*[**.***sub_if_number*]] **[force-delete** | **statistics**] [**vrf** *vrf-name* | **all** | **default** | **management**]

Syntax Description

ip-addr	(Optional) IPv4 source address. The format is x.x.x.x.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
sub_if	(Optional) Specifies the Ethernet subinterface port number. The range is from 1 to 48.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
.*sub_if_number*	(Optional) Subinterface number. The range is from 1 to 4093.
force-delete	(Optional) Clears the entries from the ARP table without a refresh.
statistics	(Optional) Clears ARP statistics.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) context name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Clears the ARP information from all VRF entries.
default	(Optional) Clears the ARP information from the default VRF.
management	(Optional) Clears the ARP information from the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear the ARP table:

```
switch# clear ip arp
```

Related Commands

Command	Description
show ip arp	Displays information about ARP.

Review Draft -- Cisco Confidential

clear ip interface statistics

To clear IP interface statistics, use the **clear ip interface statistics** command.

clear ip interface statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear the IP interface statistics:

```
switch# clear ip interface statistics
```

Related Commands

Command	Description
show ip interface	Displays IP interface information.

Review Draft -- Cisco Confidential

clear ipv6 icmp interface statistics

To clear statistics about ICMPv6, use the **clear ipv6 icmp interface statistics** command.

clear ipv6 icmp interface statistics [*type number*]

Syntax Description

type	(Optional) Interface type. Use **?** to see the list of supported interfaces.
number	(Optional) Interface number. Use **?** to see the range.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the ICMPv6 statistics:

```
switch(config-if)# clear ipv6 icmp interface statistics
```

Related Commands

Command	Description
ipv6 icmp	Configures ICMPv6 on an interface.

Review Draft -- Cisco Confidential

clear ipv6 nd interface statistics

To clear information about Neighbor Discovery (ND), use the **clear ipv6 nd interface statistics** command.

clear ipv6 nd interface statistics [*type number*]

Syntax Description

type	(Optional) Interface type. Use **?** to see the list of supported interfaces.
number	(Optional) Interface number. Use **?** to see the range.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the ND information:

```
switch(config-if)# clear ipv6 nd interface statistics
```

Related Commands

Command	Description
ipv6 nd	Configures ICMPv6 ND on an interface.

Review Draft -- Cisco Confidential

clear ipv6 neighbor

To clear IPv6 neighbors, use the **clear ipv6 neighbor** command.

clear ipv6 neighbor [*type number*] [**force-clear**] [**vrf** *vrf-name*]

Syntax Description

type	(Optional) Interface type. Use **?** to see the list of supported interfaces.
number	(Optional) Interface number. Use **?** to see the range.
force-clear	(Optional) Clears the IPv6 neighbor cache withouth a refresh.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **clear ipv6 neighbor** command to clear the IPv6 adjacency table.

This command does not require a license.

Examples

This example shows how to clear the IPv6 neighbors:

```
switch# clear ipv6 neighbor
```

Related Commands

Command	Description
ipv6 nd	Configures ICMPv6 ND on an interface.

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS Layer 3 interfaces commands that begin with I.

Review Draft -- Cisco Confidential

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address mask* [**secondary**]

no ip address *ip-address mask* [**secondary**]

Syntax Description

ip-address	IPv4 address in the format *A.B.C.D* or *A.B.C.D/length*.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration mode
Subinterface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Note Before you use this command, make sure that you use the **no switchport** command on the interface to use the Layer 3 features.

An interface can have one primary IP address and one secondary IP address.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command.

The optional **secondary** keyword allows you to specify a secondary IP address. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled, as are interface routes in the IP routing table.

Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that the secondary address of an interface fall into the same OSPF area as the primary addresses.

Examples

This example shows how to configure the IP address 192.168.0.27 as the primary address and 192.168.0.5 as the secondary address for Ethernet interface 1/5:

Review Draft -- Cisco Confidential

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 192.168.0.27 255.255.255.0
switch(config-if )# ip address 192.168.0.5 255.255.255.0 secondary
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration change to the startup configuration file.
no switchport	Enables an interface for Layer 3 configuration.
show ip interface	Displays interfaces configured for IPv4.

Review Draft -- Cisco Confidential

ip arp

To configure a static Address Resolution Protocol (ARP) entry, use the **ip arp** command. To remove a static ARP entry, use the **no** form of this command.

ip arp *ip-address mac-address*

no ip arp *ip-address*

Syntax Description

ip-address	IPv4 address, in *A.B.C.D* format.
mac-address	MAC address in one of the following formats: • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use this command on Layer 3 interfaces and Layer 3 subinterfaces.

Examples

This example shows how to configure a static ARP entry on interface Ethernet 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip arp 192.0.2.1 0150.5a03.efab
switch(config-if)#
```

This example shows how to configure a static ARP entry on a subinterface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# interface ethernet 1/1.1
switch(config-subif)# ip arp 192.0.2.1 0150.5a03.efab
switch(config-subif)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip arp	Displays ARP entries.

Review Draft -- Cisco Confidential

ip arp gratuitous

To enable gratuitous Address Resolution Protocol (ARP), use the **ip arp gratuitous** command. To disable gratuitous ARP, use the **no** form of this command.

ip arp gratuitous {**request** | **update**}

no ip arp gratuitous {**request** | **update**}

Syntax Description

request	Enables sending gratuitous ARP requests when a duplicate address is detected.
update	Enables ARP cache updates for gratuitous ARP.

Command Default

Enabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to disable gratuitous ARP request on interface Ethernet 2/1:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip arp gratuitous
switch(config-if)#
```

Related Commands

Command	Description
ip arp	Configures a static ARP entry.
show ip arp	Displays ARP configuration information.

Review Draft -- Cisco Confidential

ip arp timeout

To configure an Address Resolution Protocol (ARP) timeout, use the **ip arp timeout** command. To revert to the default value, use the **no** form of this command.

ip arp timeout *timeout-value*

no ip arp timeout

Syntax Description

timeout-value	Time (in seconds) that an entry remains in the ARP cache. Valid values are from 60 to 28800, and the default is 1500.

Command Default

1500 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to configure the ARP timeout value to 120 seconds:

```
switch(config)# ip arp timeout 120
switch(config)#
```

This example shows how to revert to the default ARP timeout value of 1500 seconds:

```
switch(config)# no ip arp timeout
switch(config)#
```

Related Commands

Command	Description
show running-config arp all	Displays the ARP configuration, including the default configurations.

Review Draft -- Cisco Confidential

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** command. To disable this function, use the **no** form of this command.

ip directed-broadcast

no ip directed-broadcast

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration mode

Subinterface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached are dropped, rather than being broadcast.

Note Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that you disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed. We also recommend that you use access lists to limit the number of broadcast packets.

Examples

This example shows how to enable forwarding of IP directed broadcasts on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
```

Review Draft -- Cisco Confidential

```
switch(config-if)# ip directed-broadcast
switch(config-if)#
```

Related Commands

Command	Description
show ip interface	Displays IP information for an interface.

Review Draft -- Cisco Confidential

interface ethernet (Layer 3)

To configure a Layer 3 Ethernet IEEE 802.3 routed interface, use the **interface ethernet** command.

interface ethernet [*chassis_ID*/] *slot*/*port*[.*subintf-port-no*]

Syntax Description

chassis_ID	(Optional) Specifies the Fabric Extender chassis ID. The chassis ID is from 100 to 199. **Note** This argument is not optional when addressing the host interfaces of a Cisco Nexus 2000 Series Fabric Extender.
slot	Slot from 1 to 3. The following list defines the slots available: • Slot 1 includes all the fixed ports. A Fabric Extender only has one slot. • Slot 2 includes the ports on the upper expansion module (if populated). • Slot 3 includes the ports on the lower expansion module (if populated).
port	Port number within a particular slot. The port number is from 1 to 128.
.	(Optional) Specifies the subinterface separator.
subintf-port-no	(Optional) Port number for the subinterface. The range is from 1 to 48.

Command Default

None

Command Modes

Global configuration mode
Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must use the **no switchport** command in the interface configuration mode to configure the interface as a Layer 3 routed interface. When you configure the interface as a Layer 3 interface, all Layer 2 specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3 specific configurations on this interface are deleted.

Examples

This example shows how to enter configuration mode for a Layer 3 Ethernet interface 1/5:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

This example shows how to enter configuration mode for a host interface on a Fabric Extender:

```
switch(config)# interface ethernet 101/1/1
```

Review Draft -- Cisco Confidential

```
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 subinterface for Ethernet interface 1/5 in the global configuration mode:

```
switch(config)# interface ethernet 1/5.2
switch(config-if)# no switchport
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```

This example shows how to configure a Layer 3 subinterface in interface configuration mode:

```
switch(config)# interface ethernet 1/5
switch(config-if)# interface ethernet 1/5.1
switch(config-if)# no switchport
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```

This example shows how to convert a Layer 3 interface to a Layer 2 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)# switchport
switch(config-if)#
```

Related Commands

Command	Description
bandwidth	Sets the bandwidth parameters for an interface.
delay	Configures the interface throughput delay value.
encapsulation	Sets the encapsulation type for an interface.
ip address	Sets a primary or secondary IP address for an interface.
inherit	Assigns a port profile to an interface.
interface vethernet	Configures a virtual Ethernet interface.
no switchport	Configures an interface as a Layer 3 interface.
service-policy	Configures a service policy for an interface.
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show interface ethernet	Displays various parameters of an Ethernet IEEE 802.3 interface.

Review Draft -- Cisco Confidential

ip local-proxy-arp

To enable the local proxy Address Resolution Protocol (ARP) feature, use the **ip local-proxy-arp** command. To disable this feature, use the **no** form of this command.

ip local-proxy-arp

no ip local-proxy-arp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode
Subinterface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before the local proxy ARP feature can be used, you must enable the IP proxy ARP feature by using the **ip proxy-arp** command. The IP proxy ARP feature is disabled by default.

Note This command is not applicable to Layer 3 loopback interfaces.

Examples

This example shows how to enable the local proxy ARP:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip arp local-proxy-arp
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
ip proxy-arp	Enables proxy ARP on an interface.
show ip arp	Displays ARP configuration information.

Review Draft -- Cisco Confidential

interface loopback

To create a loopback interface and enter interface configuration mode, use the **interface loopback** command. To remove a loopback interface, use the **no** form of this command.

interface loopback *number*

no interface loopback *number*

Syntax Description

number	Interface number; valid values are from 0 to 1023.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **interface loopback** command to create or modify loopback interfaces.

From the loopback interface configuration mode, the following parameters are available:

- **description**—Provides a description of the purpose of the interface.
- **ip**—Configures IP features, such as the IP address for the interface, Address Resolution Protocol (ARP) attributes, load balancing, Unicast Reverse Path Forwarding (RPF) or IP Source Guard.
- **logging**—Configure logging of events.
- **shutdown**—Shut down traffic on the interface.

This command does not require a license.

Examples

This example shows how to create a loopback interface:

```
switch(config)# interface loopback 50
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

Related Commands

Command	Description
show interface loopback	Displays information about the traffic on the specified loopback interface.

Review Draft -- Cisco Confidential

interface port-channel

To create an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command. To remove an EtherChannel interface, use the **no** form of this command.

interface port-channel *channel-number*[*.subintf-channel-no*]

no interface port-channel *channel-number*[*.subintf-channel-no*]

Syntax Description

channel-number	Channel number that is assigned to this EtherChannel logical interface. The range is from 1 to 4096.
.	(Optional) Specifies the subinterface separator. **Note** Applies to Layer 3 interfaces.
subintf-channel-no	(Optional) Port number of the EtherChannel subinterface. The range is from 1 to 4093. **Note** Applies to Layer 3 interfaces.

Command Default

None

Command Modes

Global configuration mode
Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

A port can belong to only one channel group.

When you use the **interface port-channel** command for Layer 2 interfaces, follow these guidelines:

- If you are using CDP, you must configure it only on the physical interface and not on the EtherChannel interface.
- If you do not assign a static MAC address on the EtherChannel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the EtherChannel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

You must use the **no switchport** command in the interface configuration mode to configure the EtherChannel interface as a Layer 3 interface. When you configure the interface as a Layer 3 interface, all Layer 2 specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 EtherChannel interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3 specific configurations on this interface are deleted.

Review Draft -- Cisco Confidential

You can configure one or more subinterfaces on a port channel made from routed interfaces.

Examples

This example shows how to create an EtherChannel group interface with channel-group number 50:

```
switch(config)# interface port-channel 50
switch(config-if)#
```

This example shows how to create a Layer 3 EtherChannel group interface with channel-group number 10:

```
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 1 in interface configuration mode:

```
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# interface port-channel 10.1
switch(config-subif)# ip address 192.0.2.2/24
switch(config-subif)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 20.1 in global configuration mode:

```
switch(config)# interface port-channel 20.1
switch(config-subif)# ip address 192.0.2.3/24
switch(config-subif)#
```

Related Commands

Command	Description
encapsulation	(Layer 3 interfaces) Sets the encapsulation type for an interface.
ip address	(Layer 3 interfaces) Sets a primary or secondary IP address for an interface.
no switchport	(Layer 3 interfaces) Configures an interface as a Layer 3 interface.
show interface	Displays configuration information about interfaces.
show lacp	Displays LACP information.
show port-channel summary	Displays information on the EtherChannels.
vtp (interface)	Enables VLAN Trunking Protocol (VTP) on an interface.

Review Draft -- Cisco Confidential

ip port-unreachable

To enable the generation of Internet Control Message Protocol (ICMP) port unreachable messages, use the **ip port-unreachable** command. To disable this function, use the **no** form of this command.

ip port-unreachable

no ip port-unreachable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration mode

Subinterface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to enable the generation of ICMP port unreachable messages, as appropriate, on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip port-unreachable
```

Related Commands

Command	Description
ip unreachables	Sends ICMP unreachable messages.

Review Draft -- Cisco Confidential

ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** command. To disable proxy ARP on the interface, use the **no** form of this command.

ip proxy-arp

no ip proxy-arp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode

Subinterface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to enable proxy ARP:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip proxy-arp
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
show ip arp	Displays ARP configuration information.

Review Draft -- Cisco Confidential

ip tcp path-mtu-discovery

To enable path maximum transmission unit (MTU) discovery on an IPv4 interface, use the **ip tcp path-mtu discovery** command. To disable this feature, use the **no** form of this command.

ip tcp path-mtu discovery

no ip tcp path-mtu discovery

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to enable path MTU discovery for IPv4:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip tcp path-mtu-discovery
switch(config-if)#
```

Related Commands

Command	Description
show ip arp	Displays ARP configuration information.

Review Draft -- Cisco Confidential

ip tcp synwait-time

To set a period of time the Cisco NX-OS software waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** command. To restore the default time, use the **no** form of this command.

ip tcp synwait-time *seconds*

no ip tcp synwait-time

Syntax Description

seconds	Time, in seconds, the software waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds.

Command Default

5 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the switch software to continue attempting to establish a TCP connection for 10 seconds:

```
switch# configure terminal
switch(config)# ip tcp synwait-time 10
Setting syn time to 10 seconds
switch(config)#
```

This example shows how to disable TCP synchronization on interfaces:

```
switch# configure terminal
switch(config)# no ip tcp synwait-time
switch(config)#
```

Related Commands

Command	Description
show running-config	Displays the running system configuration information.

Review Draft -- Cisco Confidential

ip unreachables

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachables** command. To disable this function, use the **no** form of this command.

ip unreachables

no ip unreachables

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration mode

Subinterface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to enable the generation of ICMP unreachable messages on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip unreachables
```

Related Commands

Command	Description
ip port-unreachable	Sends ICMP port unreachable messages.

Review Draft -- Cisco Confidential

ipv6 nd

To configure IPv6 neighbor discovery (ND), use the **ipv6 nd** command. To remove the IPv6 ND configuration, use the **no** form of this command.

ipv6 nd {**hop-limit** *hop-limit* | **managed-config-flag** | **mtu** | **ns-interval** *ns-interval* | **other-config-flag** | **prefix** {**A:B::C:D/LEN** | **default** {**0-4294967295** | **infinite** {**infinite** [**no-autoconfig** | **no-onlink** | **off-link**]}| **no-advertise**}} | **ra-interval** *ra-interval* | **ra-lifetime** *ra-lifetime* | **reachable-time** *reachable-time* | **redirects** | **retrans-timer** *retrans-timer* | **suppress-ra** [**mtu**]}

no ipv6 nd {**hop-limit** *hop-limit* | **managed-config-flag** | **mtu** *mtu-size* | **ns-interval** *ns-interval* | **other-config-flag** | **prefix** {**A:B::C:D/LEN** | **default** {**0-4294967295** | **infinite** {**infinite** [**no-autoconfig** | **no-onlink** | **off-link**]}| **no-advertise**}} | **ra-interval** *ra-interval* | **ra-lifetime** *ra-lifetime* | **reachable-time** *reachable-time* | **redirects** | **retrans-timer** *retrans-timer* | **suppress-ra** [**mtu**]}

Syntax Description

hop-limit	Specifies the hop limit in the IPv6 header.
hop-limit	Hop limit. The range is from 0 to 255.
managed-config-flag	Informs hosts to use stateful address autoconfiguration to obtain address information.
mtu	Specifies the MTU size.
mtu-size	MTU size. The range is from 1280 to 65535.
ns-interval	Specifies the retransmission interval between sending the neighbor-solicitation messages.
ns-interval	Interval in milliseconds. The range is from 1000 to 3600000.
other-config-flag	Informs hosts to use stateful autoconfiguration to obtain non-address related information.
prefix	Specifies the IPv6 prefix to advertise in the router-advertisement message.
A:B::C:D/LEN	Specifies the IPv6 address prefix.
default	Specifies the prefix default parameters.
0-4294967295	Valid value for the life time.
infinite	Specifies the indefinite lifetime.
no-autoconfig	(Optional) Specifies no to use the prefix for autoconfiguration.
no-onlink	(Optional) Specifies not use the prefix for the onlink determination.
off-link	Indicates the prefix is offlink.
no-advertise	Specifies not to advertise the prefix.
ra-interval	Specifies the interval between sending the router-advertisement message.
ra-interval	Router-advertisement message interval. The range is from 4 to 1800.
ra-lifetime	Specifies the router lifetime of a default router.
ra-lifetime	Router-advertisement message lifetime. The range is from 4 to 1800. The value for the default router cannot be 0.
reachable-time	Specifies the advertised time when a node considers a neighbor is up after receiving a reachability confirmation.
reachable-time	Reachable time. The range is from 0 to 3600000.

Review Draft -- Cisco Confidential

redirects	Enables sending ICMPv6 Redirect messages.
retrans-timer	Specifies the advertised time between NS messages.
retrans-timer	Time between messages. The range is from 0 to 4294967295.
suppress-ra	Disables sending router-advertisement messages.

Defaults

hop-limit–64
mtu–1500
ns-interval–1000
ra-interval–600
reachable-time–0
retrans-timer–0

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure IPv6 neighbor discovery:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ipv6 nd
switch(config-if)# ipv6 nd reachable time 30
```

This example shows how to remove IPv6 neighbor discovery:

```
switch(config-if)# no ipv6 nd reachable time 30
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 nd interface	Displays neighbor discovery interface information.

Review Draft -- Cisco Confidential

N Commands

This chapter describes the Cisco NX-OS Layer 3 interfaces commands that begin with N.

Review Draft -- Cisco Confidential

no switchport

To configure the interface as a Layer 3 Ethernet interface, use the **no switchport** command.

no switchport

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can configure any Ethernet port as a routed interface. When you configure an interface as a Layer 3 interface, any configuration specific to Layer 2 on this interface is deleted.

If you want to configure a Layer 3 interface for Layer 2, enter the **switchport** command. Then, if you change a Layer 2 interface to a routed interface, enter the **no switchport** command.

Examples

This example shows how to enable an interface as a Layer 3 routed interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)#
```

This example shows how to configure a Layer 3 interface as a Layer 2 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
ip address	Sets a primary or secondary IP address for an interface.
show interfaces	Displays interface information.

Review Draft -- Cisco Confidential

R Commands

This chapter describes the Cisco NX-OS Layer 3 interfaces commands that begin with R.

Review Draft -- Cisco Confidential

routing-context vrf

To set the virtual routing and forwarding (VRF) scope for all EXEC commands, use the **routing-context vrf** command. To return to the default setting, use the **no** form of this command.

routing-context vrf *vrf-name*

no routing-context vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF instance. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

default VRF

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **routing-context vrf** command to set the VRF scope for all EXEC commands (for example, **show** commands). This feature automatically restricts the scope of the output of EXEC commands to the configured VRF. You can override this scope by using the VRF keywords available for some EXEC commands.

Examples

This example shows how to limit EXEC commands to the management VRF:

```
switch# routing-context vrf management
switch%management#
```

Related Commands

Command	Description
show routing-context	Displays the current routing context.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS Layer 3 interfaces **show** commands.

Review Draft -- Cisco Confidential

show interface brief

To display a brief summary of the interface configuration information, use the **show interface brief** command.

show interface brief

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the summary configuration information of the specified interface:

```
switch# show interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                 Ch #
--------------------------------------------------------------------------------
Eth1/1        1      eth  trunk  up      none                       10G(D) 4000
Eth1/2        1      eth  trunk  up      none                       10G(D) 4000
Eth1/3        1      eth  trunk  up      none                       10G(D) 4000
Eth1/4        1      eth  trunk  up      none                       10G(D) 4000
Eth1/5        1      eth  access down    SFP not inserted           10G(D) --
Eth1/6        1      eth  access down    SFP not inserted           10G(D) --
Eth1/7        1      eth  trunk  up      none                       10G(D) 10
Eth1/8        1      eth  trunk  up      none                       10G(D) 10
Eth1/9        1      eth  trunk  up      none                       10G(D) 10
Eth1/10       1      eth  trunk  up      none                       10G(D) 10
Eth1/11       1      eth  access down    SFP not inserted           10G(D) --
Eth1/12       1      eth  access down    SFP not inserted           10G(D) --
Eth1/13       1      eth  access down    SFP not inserted           10G(D) --
Eth1/14       1      eth  access down    SFP not inserted           10G(D) --
Eth1/15       1      eth  access down    SFP not inserted           10G(D) --
Eth1/16       1      eth  access down    SFP not inserted           10G(D) --
Eth1/17       1      eth  access down    SFP not inserted           10G(D) --
Eth1/18       1      eth  access down    SFP not inserted           10G(D) --
Eth1/19       1      eth  access down    SFP not inserted           10G(D) --
Eth1/20       1      eth  access down    SFP not inserted           10G(D) --
Eth1/21       1      eth  access down    SFP not inserted           10G(D) --
Eth1/22       1      eth  access down    SFP not inserted           10G(D) --
Eth1/23       1      eth  access down    Link not connected         10G(D) --
Eth1/24       1      eth  access down    Link not connected         10G(D) --
Eth1/25       1      eth  access down    SFP not inserted           10G(D) --
Eth1/26       1      eth  access down    SFP not inserted           10G(D) --
Eth1/27       1      eth  access down    SFP not inserted           10G(D) --
```

Review Draft -- Cisco Confidential

```
Eth1/28       1      eth  access down    SFP not inserted            10G(D) --
Eth1/29       1      eth  access down    SFP not inserted            10G(D) --
Eth1/30       1      eth  access down    SFP not inserted            10G(D) --
Eth1/31       1      eth  access down    SFP not inserted            10G(D) --
Eth1/32       1      eth  access down    SFP not inserted            10G(D) --
Eth1/33       1      eth  access down    SFP not inserted            10G(D) --
Eth1/34       1      eth  access down    SFP not inserted            10G(D) --
Eth1/35       1      eth  access down    SFP not inserted            10G(D) --
Eth1/36       1      eth  access down    SFP not inserted            10G(D) --
Eth1/37       1      eth  access down    SFP not inserted            10G(D) --
Eth1/38       1      eth  access down    SFP not inserted            10G(D) --
Eth1/39       1      eth  access down    SFP not inserted            10G(D) --
Eth1/40       1      eth  trunk  up      none                        10G(D) --
Eth2/1        1      eth  access down    SFP not inserted            10G(D) --
Eth2/2        1      eth  access up      none                        10G(D) --
Eth2/3        1      eth  access down    SFP not inserted            10G(D) --
Eth2/4        1      eth  access up      none                        10G(D) --
Eth2/5        1      eth  access up      none                        10G(D) --
Eth2/6        1      eth  access down    SFP not inserted            10G(D) --

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                   Speed  Protocol
Interface
--------------------------------------------------------------------------------
Po10         1     eth  trunk  up      none                      a-10G(D)  lacp
Po4000       1     eth  trunk  up      none                      a-10G(D)  lacp

--------------------------------------------------------------------------------
Port   VRF           Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --            up     192.168.10.37                           100      1500

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                    Status Reason
--------------------------------------------------------------------------------
Vlan1     --                                      down   Administratively down

switch#
```

This example shows how to display the summary configuration information of interfaces, including routed interfaces:

```
switch# show interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth1/1        1      eth  access down    Link not connected          10G(D) --
Eth1/2        1      eth  trunk  up      none                        10G(D) --
Eth1/3        1      eth  access down    SFP not inserted            10G(D) --
Eth1/4        1      eth  access down    SFP not inserted            10G(D) --
Eth1/5        --     eth  routed up      none                        10G(D) --
Eth1/5.2      --     eth  routed down    Configuration Incomplete    10G(D) --
Eth1/6        1      eth  access up      none                        10G(D) --
Eth1/7        1      eth  access up      none                        10G(D) --
Eth1/8        1      eth  trunk  up      none                        10G(D) 100
Eth1/9        1      eth  access up      none                        10G(D) --
Eth1/10       1      eth  access down    Link not connected          10G(D) --
Eth1/11       1      eth  access down    SFP not inserted            10G(D) --
Eth1/12       1      eth  access down    SFP not inserted            10G(D) --
Eth1/13       1      eth  access down    SFP not inserted            10G(D) --
Eth1/14       1      eth  access down    SFP not inserted            10G(D) --
Eth1/15       1      eth  access down    SFP not inserted            10G(D) --
```

Review Draft -- Cisco Confidential

```
Eth1/16       1       eth  access down    SFP not inserted           10G(D) --
Eth1/17       1       eth  access up      none                       10G(D) --
Eth1/18       1       eth  access up      none                       10G(D) --
Eth1/19       1       eth  fabric up      none                       10G(D) --
Eth1/20       1       eth  access down    Link not connected         10G(D) --
Eth1/21       1       eth  access up      none                       10G(D) --
Eth1/22       1       eth  access down    Link not connected         10G(D) --
Eth1/23       1       eth  access down    SFP not inserted           10G(D) --
Eth1/24       1       eth  access down    SFP not inserted           10G(D) --
Eth1/25       1       eth  access down    Link not connected         10G(D) --
Eth1/26       1       eth  access down    SFP not inserted           10G(D) --
Eth1/27       1       eth  access down    SFP not inserted           10G(D) --
Eth1/28       1       eth  access down    SFP not inserted           10G(D) --
Eth1/29       1       eth  access down    Link not connected         10G(D) --
Eth1/30       1       eth  access down    SFP not inserted           10G(D) --
Eth1/31       1       eth  access down    SFP not inserted           10G(D) --
Eth1/32       1       eth  access up      none                       10G(D) --

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                   Speed  Protocol
Interface
--------------------------------------------------------------------------------
Po100        1     eth  trunk  up      none                     a-10G(D)  none

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     172.29.231.33                           1000     1500

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                    Status Reason
--------------------------------------------------------------------------------
Vlan1     --                                      up     --
Vlan100   --                                      up     --

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth100/1/1    1       eth  access up      none                       10G(D) --
Eth100/1/2    1       eth  access down    Link not connected       auto(D) --
Eth100/1/3    1       eth  access up      none                       10G(D) --
Eth100/1/4    1       eth  access down    Link not connected       auto(D) --
Eth100/1/5    1       eth  access down    Link not connected       auto(D) --
Eth100/1/6    1       eth  access down    Link not connected       auto(D) --
Eth100/1/7    1       eth  access down    Link not connected       auto(D) --
Eth100/1/8    1       eth  access down    Link not connected       auto(D) --
Eth100/1/9    1       eth  access down    Link not connected       auto(D) --
Eth100/1/10   1       eth  access up      none                       10G(D) --
Eth100/1/11   1       eth  access down    Link not connected       auto(D) --
Eth100/1/12   1       eth  access down    Link not connected       auto(D) --
Eth100/1/13   1       eth  access down    Link not connected       auto(D) --
Eth100/1/14   1       eth  access down    Link not connected       auto(D) --
Eth100/1/15   1       eth  access up      none                       10G(D) --
Eth100/1/16   1       eth  access down    Link not connected       auto(D) --

--------------------------------------------------------------------------------
Interface     Status     Description
--------------------------------------------------------------------------------
Lo10          up         --
switch#
```

Note the following in the above display:

Review Draft -- Cisco Confidential

- Ethernet 1/5 is a Layer 3-ready interface. The following fields in the display help identify an interface as a configured Layer 3 interface:
  - Mode—routed
  - Status—up
  - Reason—none
- Ethernet 1/5.2 is a Layer 3 subinterface; however, the interface is not ready for Layer 3 configuration (Status—down).
- Interface Lo10 is a Layer 3 loopback interface.

This example shows how to display a brief summary of interfaces configured as FabricPath interfaces on a switch that runs Cisco Nexus 6000 Release 6.0(2)N1(1):

Need new output

```
switch# show interface brief
--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch#
--------------------------------------------------------------------------------
Eth1/1        1       eth  access down    SFP not inserted           1000(D) --
Eth1/2        --      eth  routed down    SFP not inserted           1000(D) --
Eth1/3        1       eth  access down    SFP not inserted            10G(D) --
Eth1/4        1       eth  access down    SFP not inserted            10G(D) --
Eth1/5        1       eth  f-path down    SFP not inserted            10G(D) --
Eth1/6        1       eth  access down    Link not connected          10G(D) --
Eth1/7        1       eth  fabric down    Link not connected          10G(D) --
Eth1/8        1       eth  access down    SFP not inserted            10G(D) --
Eth1/9        1       eth  access down    SFP not inserted            10G(D) --
Eth1/10       1       eth  access down    SFP not inserted            10G(D) --
Eth1/11       1       eth  access down    SFP not inserted            10G(D) --
Eth1/12       1       eth  access down    SFP not inserted            10G(D) --
Eth1/13       1       eth  access down    SFP not inserted            10G(D) --
Eth1/14       1       eth  access down    SFP not inserted            10G(D) --
Eth1/15       1       eth  pvlan  up      none                       1000(D) --
Eth1/16       1       eth  access down    SFP not inserted            10G(D) --
Eth1/17       1       eth  access down    SFP not inserted            10G(D) --
switch#
```

In the above display, Ethernet 1/5 has the mode shown as “f-path” indicating that it has been configured as a FabricPath port.

Related Commands

Command	Description
interface ethernet	Configures an Ethernet IEEE 802.3 interface.

Review Draft -- Cisco Confidential

show interface ethernet

To display information about the interface configuration, use the **show interface ethernet** command.

show interface ethernet *slot/port*[*.subintf-port-no*] [**brief** | **counters** | **description** | **status** | **switchport**]

Syntax Description

slot/port	Ethernet interface slot number and port number. The *slot* number is from 1 to 255, and the *port* number is from 1 to 128.
.	(Optional) Specifies the subinterface separator. **Note** This keyword applies to Layer 3 interfaces.
subintf-port-no	(Optional) Port number for the subinterface. The range is from 1 to 48. **Note** This argument applies to Layer 3 interfaces.
brief	(Optional) Displays brief information about the interfaces.
counters	(Optional) Displays information about the counters configured on an interface.
description	(Optional) Displays the description of an interface configuration.
status	(Optional) Displays the operational state of the interface.
switchport	(Optional) Displays the switchport information of an interface.

Command Default

Displays all information for the interface.

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the detailed configuration of the specified interface:

```
switch# show interface ethernet 1/1
Ethernet1/1 is up
  Hardware: 1000/10000 Ethernet, address: 000d.ece7.df48 (bia 000d.ece7.df48)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is fex-fabric
  full-duplex, 10 Gb/s, media type is 1/10g
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Switchport monitor is off
  Last link flapped 09:03:57
  Last clearing of "show interface" counters never
  30 seconds input rate 2376 bits/sec, 0 packets/sec
  30 seconds output rate 1584 bits/sec, 0 packets/sec
```

Review Draft -- Cisco Confidential

```
  Load-Interval #2: 5 minute (300 seconds)
    input rate 1.58 Kbps, 0 pps; output rate 792 bps, 0 pps
  RX
    0 unicast packets  10440 multicast packets  0 broadcast packets
    10440 input packets  11108120 bytes
    0 jumbo packets  0 storm suppression packets
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    0 unicast packets  20241 multicast packets  105 broadcast packets
    20346 output packets  7633280 bytes
    0 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble
    0 Tx pause
  1 interface resets

switch#
```

This example shows how to display the counters configured on a specified interface:

```
switch# show interface ethernet 1/1 counters

--------------------------------------------------------------------------------
Port                InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
Eth1/1              17193136                 0            16159                0
--------------------------------------------------------------------------------
Port               OutOctets      OutUcastPkts     OutMcastPkts     OutBcastPkts
--------------------------------------------------------------------------------
Eth1/1           11576758                 0            28326              106
switch#
```

This example shows how to display the detailed configuration information of a specified subinterface:

```
switch# show interface ethernet 1/5.2
Ethernet1/5.2 is up
  Hardware: 1000/10000 Ethernet, address: 0005.73a6.1dbc (bia 0005.73a6.1d6c)
  Description: Eth 1/5.2 subinterfaces
  Internet Address is 192.0.0.3/24
  MTU 1500 bytes, BW 1500 Kbit, DLY 2000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 100
  EtherType is 0x8100

switch#
```

This example shows how to display the brief configuration information of a specified subinterface:

```
switch# show interface ethernet 1/5.2 brief

--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth1/5.2      100     eth  routed up      none                       10G(D) --
switch#
```

This example shows how to display the purpose of a specified subinterface:

```
switch# show interface ethernet 1/5.2 description
```

Review Draft -- Cisco Confidential

```
--------------------------------------------------------------------------------
Port          Type   Speed   Description
--------------------------------------------------------------------------------
Eth1/5.2      eth    10G     Eth 1/5.2 subinterfaces
switch#
```

Related Commands

Command	Description
interface ethernet	Configures an Ethernet IEEE 802.3 interface.
interface ethernet (Layer 3)	Configures a Layer 3 Ethernet IEEE 802.3 interface.
switchport mode vntag	Configures an Ethernet interface as a VNTag port.
switchport monitor rate-limit	Configures the rate limit for traffic on an interface.

Review Draft -- Cisco Confidential

show interface loopback

To display information about the loopback interface, use the **show interface loopback** command.

show interface loopback *lo-number* [**brief** | **description**]

Syntax Description

lo-number	Loopback interface number. The range is from 0 to 1023.
brief	(Optional) Displays a brief summary of the loopback interface information.
description	(Optional) Displays the description provided for the loopback interface.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the configuration information for a specific loopback interface:

```
switch# show interface loopback 10
loopback10 is up
  Hardware: Loopback
  MTU 1500 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK
    0 packets input 0 bytes
    0 multicast frames 0 compressed
    0 input errors 0 frame 0 overrun 0 fifo
    0 packets output 0 bytes 0 underruns
    0 output errors 0 collisions 0 fifo

switch#
```

Table 1 describes the significant fields shown in the display.

Table 1 show interface loopback Field Description

Field	Description
Loopback is ...	Indicates whether the interface hardware is currently active (whether carrier detect is present), is currently inactive (down), or has been taken down by an administrator (administratively down).
Hardware	Hardware is Loopback.
MTU	Maximum transmission unit (MTU) of the interface.
BW	Bandwidth (BW) of the interface in kilobits per second.
DLY	Delay (DLY) of the interface in microseconds.

Review Draft -- Cisco Confidential

Table 1 show interface loopback Field Description (continued)

Field	Description
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Load on the interface for transmitting packets as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Load on the interface for receiving packets as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
LOOPBACK	Indicates whether loopback is set.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
multicast frames	Total number of multicast frames enabled on the interface.
compressed	Total number of multicast frames compressed on the interface.
input errors	Sum of all errors that prevented the receipt of datagrams on the interface being examined. This may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
fifo	Number of First In, First Out (FIFO) errors in the receive direction.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle. This may never happen (be reported) on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Loopback interface does not have collisions.
fifo	Number of First In, First Out (FIFO) errors in the transmit direction.

Review Draft -- Cisco Confidential

This example shows how to display the brief information for a specific loopback interface:

```
switch# show interface loopback 10 brief

--------------------------------------------------------------------------------
Interface     Status     Description
--------------------------------------------------------------------------------
loopback10    up         --
switch#
```

Related Commands

Command	Description
interface loopback	Configures a loopback interface.

Review Draft -- Cisco Confidential

show interface port-channel

To display the information about an EtherChannel interface configuration, use the **show interface port-channel** command.

show interface port-channel *number*[**.***subinterface-number*] [**brief | counters | description | status**]

Syntax Description

number	EtherChannel number. The range is from 1 to 4096.
.*subinterface-number*	(Optional) Port-channel subinterface configuration. Use the EtherChannel number followed by a dot (.) indicator and the subinterface number. The format is: *portchannel-number.subinterface-number*
counters	(Optional) Displays information about the counters configured on the EtherChannel interface.
description	(Optional) Displays the description of the EtherChannel interface configuration.
status	(Optional) Displays the operational state of the EtherChannel interface.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the configuration information of a specified EtherChannel interface:

```
switch# show interface port-channel 21
port-channel21 is up
  Hardware: Port-Channel, address: 000d.ece7.df72 (bia 000d.ece7.df72)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s
  Beacon is turned off
  Input flow-control is on, output flow-control is on
  Switchport monitor is off
  Members in this channel: Eth2/3
  Last clearing of "show interface" counters never
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 352 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 368 bps, 0 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast packets
```

Review Draft -- Cisco Confidential

```
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression packets
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    0 unicast packets  15813 multicast packets  9 broadcast packets
    15822 output packets  1615917 bytes
    0 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble
    0 Tx pause
  1 interface resets

switch#
```

Related Commands

Command	Description
interface port-channel	Configures an EtherChannel interface.

Review Draft -- Cisco Confidential

show ip arp

To display the Address Resolution Protocol (ARP) information, use the **show ip arp** command.

show ip arp [*ip-addr* | {**ethernet** *slot/port* | **loopback** *if_number* | **mgmt** *mif_number* | **port-channel** *number*}] [**client**] [**static**] [**statistics**] [**vrf** *vrf-name*]

Syntax Description

ip-addr	(Optional) IPv4 source address. The format is x.x.x.x.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
mgmt *mif_number*	(Optional) Specifies the management interface. The management interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
client	(Optional) Displays the ARP client table
static	(Optional) Displays static ARP entries.
statistics	(Optional) Displays ARP statistics.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the ARP information:

```
switch# show ip arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 1
Address         Age       MAC Address     Interface
2.2.2.100         -       000a.000a.000a  Ethernet1/2
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
ip arp	Configures a static ARP entry.

Review Draft -- Cisco Confidential

show ip arp summary

To display ARP adjacency summary, use the **show ip arp summary** command.

show ip arp summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display ARP adjacency summary:

```
switch# show ip arp summary

IP ARP Table - Adjacency Summary

  Resolved   : 0
  Incomplete : 0
  Unknown    : 0
  Total      : 0

switch#
```

Related Commands

Command	Description
ip arp timeout	Configures ARP.

Review Draft -- Cisco Confidential

show ip client

To display information about the internal IP clients, use the **show ip client** command.

show ip client [*name*]

Syntax Description

name	(Optional) Name of the client.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the IP client information for the Address Resolution Protocol (ARP):

```
switch(config)# show ip client arp
```

Related Commands

Command	Description
show ip process	Displays information about the IP process.

Review Draft -- Cisco Confidential

show ip interface

To display IP information for an interface, use the **show ip interface** command.

show ip interface [*type number*] [**brief**] [**vrf** *vrf-name*]

Syntax Description

type	(Optional) Interface type. Use **?** to see the options.
number	(Optional) Interface number. Use **?** to see the range.
brief	(Optional) Displays a summary of IP information.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the IP information for Ethernet 1/5:

```
switch# show ip interface ethernet 1/5
IP Interface Status for VRF "default"(1)
Ethernet1/5, Interface status: protocol-down/link-down/admin-up, iod: 11,
  IP address: 192.0.0.1, IP subnet: 192.0.0.0/24
  IP broadcast address: 255.255.255.255
  IP multicast groups locally joined: none
  IP MTU: 1500 bytes (using link MTU)
  IP primary address route-preference: 0, tag: 0
  IP proxy ARP : disabled
  IP Local Proxy ARP : disabled
  IP multicast routing: disabled
  IP icmp redirects: enabled
  IP directed-broadcast: disabled
  IP icmp unreachables (except port): disabled
  IP icmp port-unreachable: enabled
  IP unicast reverse path forwarding: none
  IP load sharing: none
  IP interface statistics last reset: never
  IP interface software stats: (sent/received/forwarded/originated/consumed)
    Unicast packets      : 0/0/0/0/0
    Unicast bytes        : 0/0/0/0/0
    Multicast packets    : 0/0/0/0/0
    Multicast bytes      : 0/0/0/0/0
    Broadcast packets    : 0/0/0/0/0
    Broadcast bytes      : 0/0/0/0/0
```

Review Draft -- Cisco Confidential

```
    Labeled packets     : 0/0/0/0/0
    Labeled bytes       : 0/0/0/0/0
switch#
```

Related Commands

Command	Description
ip address	Assigns a primary IP address for a network interface.

Review Draft -- Cisco Confidential

show running-config arp

To display the Address Resolution Protocol (ARP) configuration in the running configuration, use the **show running-config arp** command.

show running-config arp [**all**]

Syntax Description		
	all	(Optional) Displays configured and default information.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

Examples This example shows how to display the ARP configuration:

Need new output

```
switch# show running-config arp

!Command: show running-config arp
!Time: Mon Aug 23 07:33:15 2010

version 5.0(2)N1(1)
ip arp timeout 2100
ip arp event-history errors size medium

interface Vlan10
  ip arp 192.0.11.37 00C0.4F00.0000

switch#
```

This example shows how to display the ARP configuration with the default information:

```
switch# show running-config arp all

!Command: show running-config arp all
!Time: Mon Aug 23 07:33:52 2010

version 5.0(2)N1(1)
ip arp timeout 1500
ip arp event-history cli size small
ip arp event-history snmp size small
ip arp event-history client-errors size small
ip arp event-history client-event size small
ip arp event-history lcache-errors size small
ip arp event-history lcache size small
ip arp event-history errors size small
```

Review Draft -- Cisco Confidential

```
ip arp event-history ha size small
ip arp event-history event size small
ip arp event-history packet size small

interface Vlan10
  ip arp 192.0.11.37 00C0.4F00.0000
  ip arp gratuitous update
  ip arp gratuitous request

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration file.
ip arp timeout	Configures an ARP timeout.
show startup-config arp	Displays the ARP startup configuration.

Review Draft -- Cisco Confidential

show startup-config arp

To display the Address Resolution Protocol (ARP) configuration in the startup configuration, use the **show startup-config arp** command.

show startup-config arp [**all**]

Syntax Description		
	all	(Optional) Displays configured and default information.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

Examples This example shows how to display the ARP startup configuration:

Need new output

```
switch# show startup-config arp

!Command: show running-config arp
!Time: Mon Aug 23 07:33:15 2010

version 5.0(2)N1(1)
ip arp timeout 2100
ip arp event-history errors size medium

interface Vlan10
  ip arp 192.0.1.37 00C0.4F00.0000

switch#
```

Related Commands	Command	Description
	copy running-config startup-config	Copies the running configuration to the startup configuration file.
	ip arp timeout	Configures an ARP timeout.
	show running-config arp	Displays the ARP running configuration.

<l_Italic>Review Draft -- Cisco Confidential

PART 10

Object Tracking Commands

Review Draft -- Cisco Confidential

D Commands

This chapter describes the Cisco NX-OS object tracking commands that begin with D.

Review Draft -- Cisco Confidential

delay

To delay a state change for object tracking, use the **delay** command. To disable this function, use the **no** form of this command.

delay {**up** *up-time* [**down** *down-time*] | **down** *down-time* [**up** *up-time*]}

no delay

Syntax Description

up *up-time*	Delays the object track state change for an up condition. The range is from 0 to 180 seconds.
down *down-time*	Delays the object track state change for a down condition. The range is from 0 to 180 seconds.

Command Default

None

Command Modes

Object track mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **delay** command to delay when object tracking detects an up or down state change for a tracked object or track list. This delay helps to prevent state flapping.

Examples

This example shows how to configure the delay timer for a tracked object:

```
switch(config)# configure terminal
switch(config)# track 1 interface ethernet 1/2 line-protocol
switch(config-track)# delay up 30 down 30
switch(config-track)#
```

Related Commands

Command	Description
track	Configures a tracked object or track list.

Review Draft -- Cisco Confidential

O Commands

This chapter describes the Cisco NX-OS object tracking commands that begin with O.

Review Draft -- Cisco Confidential

object

To specify an object for a tracked list, use the **object** command. To remove the object from the tracked list, use the **no** form of this command.

object *object-number* [**not**] [**weight** *weight-number*]

no object *object-number*

Syntax Description

not	(Optional) Negates the state of an object. **Note** You cannot use the **not** keyword in a weight or percentage threshold list. You can use this keyword only in a Boolean list.
weight *weight-number*	(Optional) Specifies a threshold weight for each object.

Command Default

None

Command Modes

Tracking configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can configure an object track list that contains multiple tracked objects. A tracked list contains one or more objects.

The Boolean expression enables two types of calculation by using either "and" or "or" operators.

You can also configure an object track list that contains a percentage threshold.The percentage of up objects must exceed the configured track list up percent threshold before the track list is in an up state. For example, if the tracked list has three objects, and you configure an up threshold of 60 percent, two of the objects must be in the up state (66 percent of all objects) for the track list to be in the up state.

You can also configure an object track list that contains a weight threshold. A tracked list contains one or more objects. The combined weight of up objects must exceed the configured track list up weight threshold before the track list is in an up state. For example, if the tracked list has three objects with the default weight of 10 each, and you configure an up threshold of 15, two of the objects must be in the up state (combined weight of 20) for the track list to be in the up state.

Examples

This example shows how to configure a track list with an up weight threshold of 30 and a down threshold of 10:

```
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
```

Review Draft -- Cisco Confidential

```
switch(config-track)# object 30
switch(config-track)#
```

Related Commands

Command	Description
track list	Configures a track list for object tracking.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS object tracking **show** commands.

Review Draft -- Cisco Confidential

show track

To show information about object tracking, use the **show track** command.

show track [*object-id*] [**interface** | **ip route**] [**brief**]

Syntax Description

object-id	(Optional) Tracking ID. The range can be from 1 to 500.
interface	(Optional) Displays information about tracked interfaces.
ip route	(Optional) Displays information about tracked IP routes.
brief	(Optional) Displays brief information about tracked objects.

Command Default

Display information for all tracked objects.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display information about tracked interfaces:

```
switch# show track interface
```

This example shows how to display information about tracked IP routes:

```
switch# show track ip route
```

This example shows how to display brief information about tracked objects:

```
switch# show track brief
```

Related Commands

Command	Description
track interface	Tracks the state of an interface.
track ip route	Tracks the state of an IP route.

Review Draft -- Cisco Confidential

T Commands

This chapter describes the Cisco NX-OS object tracking commands that begin with T.

Review Draft -- Cisco Confidential

threshold percentage

To set a threshold percentage for a tracked object in a list of objects, use the **threshold percentage** command. To disable the threshold percentage, use the **no** form of this command.

threshold percentage {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}

no threshold percentage

Syntax Description

up	Specifies the up threshold.
down	(Optional) Specifies the down threshold.
number	Threshold value. The range is from 0 to 100.

Command Default

None

Command Modes

Tracking configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

When you configure a tracked list using the **track** *object-number* **list** command, there are two keywords available: **boolean** and **threshold**. If you specify the **threshold** keyword, you can specify either the **percentage** or **weight** keywords. If you specify the **percentage** keyword, the **weight** keyword is unavailable. If you specify the **weight** keyword, the **percentage** keyword is unavailable.

You should configure the up percentage first. The valid range is from 1 to 100. The down percentage depends on what you have configured for up. For example, if you configure 50 percent for up, you see a range from 0 to 49 percent for down.

Examples

This example shows how to configure the tracked list 11 to measure the threshold using an up percentage of 50 and a down percentage of 32:

```
switch(config)# track 11 list threshold percentage
switch(config-track)# object 1
switch(config-track)# object 2
switch(config-track)# threshold percentage up 50 down 32
switch(config-track)#
```

Related Commands

Command	Description
threshold weight	Sets a threshold weight for a tracked object in a list of objects.
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.

Review Draft -- Cisco Confidential

threshold weight

To set a threshold weight for a tracked object in a list of objects, use the **threshold weight** command. To disable the threshold weight, use the **no** form of this command.

threshold weight {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}

no threshold weight

Syntax Description

up	Specifies the up threshold.
down	(Optional) Specifies the down threshold.
number	Threshold value. The range is from 1 to 255.

Command Default

None

Command Modes

Tracking configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

When you configure a tracked list using the **track** *object-number* **list** command, there are two keywords available: **boolean** and **threshold**. If you specify the **threshold** keyword, you can specify either the **percentage** or **weight** keywords. If you specify the **percentage** keyword, the **weight** keyword is unavailable. If you specify the **weight** keyword, the **percentage** keyword is unavailable.

You should configure the up weight first. The valid range is from 1 to 255. The available down weight depends on what you have configured for the up weight. For example, if you configure 25 for up, you will see a range from 0 to 24 for down.

Examples

This example shows how to configure the tracked list 12 to measure a threshold using a specified weight:

```
switch(config)# track 11 list threshold weight
switch(config-track)# object 1
switch(config-track)# object 2
switch(config-track)# threshold weight up 35 down 22
switch(config-track)#
```

Related Commands

Command	Description
threshold percentage	Sets a threshold percentage for a tracked object in a list of objects.
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.

Review Draft -- Cisco Confidential

track interface

To configure object tracking on an interface, use the **track interface** command. To remove the object tracking for this interface, use the **no** form of this command.

track *object-id* **interface** *interface-type number* {**ip routing** | **line-protocol**}

no track *object-id* [**force**]

Syntax Description

object-id	Tracking ID. The range can be from 1 to 500.
interface *interface-type number*	Specifies the interface to track. Use the online ? help to see a list of available interface types.
ip routing	Tracks the IP routing state of the interface.
line-protocol	Tracks the line protocol state of the interface.
force	(Optional) Completely removes the object tracking instance.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **track interface** command to track the line protocol status or IPv4 routing state of an interface. This command enters the object tracking command mode. Use the **vrf member** command in object tracking configuration mode to track objects in a nondefault VRF.

Examples

This example shows how to track the IP routing state on interface Ethernet 1/2:

```
switch(config)# track 1 interface ethernet 1/2 ip routing
switch(config-track)#
```

Related Commands

Command	Description
show track	Displays information about object tracking.
track ip route reachability	Tracks the state of an IPv4 route reachability.
vrf member	Tracks an object in a nondefault VRF.

Review Draft -- Cisco Confidential

track ip route

To configure object tracking on an IP route, use the **track ip route** command. To remove the object tracking for this route, use the **no** form of this command.

track *object-id* **ip route** *ip-prefix/length* **reachability**

no track *object-id* [**force**]

Syntax Description

object-id	Tracking ID. The range can be from 1 to 500.
ip-prefix/length	Prefix of route to track. The IP prefix is in dotted decimal format (X.X.X.X). The length can be from 1 to 32.
reachability	Tracks the reachability state of an IP route.
force	(Optional) Completely removes the object tracking instance.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **track ip route** command to track IP route reachability. This command enters the object tracking command mode. Use the **vrf member** command in object tracking configuration mode to track objects in a nondefault VRF.

Examples

This example shows how to track an IP route:

```
switch(config)# track 1 ip route 10.10.10.0/8 reachability
switch(config-track)#
```

Related Commands

Command	Description
show track	Displays information about object tracking.
track interface	Tracks an interface.
vrf member	Tracks an object in a nondefault VRF.

Review Draft -- Cisco Confidential

track list

To configure object tracking on an object list, use the **track list** command. To remove the object tracking for this object list, use the **no** form of this command.

track *object-id* **list boolean** {**and** | **or**}

track *object-id* **list threshold** {**percentage** | **weight**}

no track *object-id* [**force**]

Syntax Description

object-id	Tracking ID. The range can be from 1 to 500.
boolean	Combines the tracked object states as a boolean combination.
and	Combines the tracked object states as a boolean AND.
or	Combines the tracked object states as a boolean OR.
threshold	Combines the tracked object states as a percent or weight combination.
percentage	Combines the tracked object states as a percent of the total number of tracked objects in the list.
weight	Combines the tracked object states as a combination of their configured weights.
force	(Optional) Completely removes the object tracking instance.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **track list** command to create a list of objects to combine into one tracked state. Use the **boolean and** keywords to combine the tracked objects as an AND function (that is, all objects must be up for the track list to be up). Use the **boolean or** keywords to combine the tracked objects as an OR (that is if any object is up, the tracked state is up).

The track list command enters the track command mode. You can configure the following commands in this mode:

- **object**—Configures one or more objects to track in the track list. You can optionally use the **not** keyword to negate the object track state. (That is, an up state becomes a down state if you use the **not** keyword) for boolean tracked lists. You can optionally use the **weight** keyword to assign a weight to an object for a threshold weight tracked list. The default weight is 10.
- **vrf**—Assigns the track list to a VRF.

Review Draft -- Cisco Confidential

Examples

This example shows how to create a track list of two objects and AND their state:

```
switch# configure terminal
switch(config)# track 1 boolean and
switch(config-track)# object 33
switch(config-track)# object 30
switch(config-track)#
```

This example shows how to configure a track list with an up threshold of 70 percent and a down threshold of 30 percent:

```
switch# configure terminal
switch(config)# track 1 list threshold percentage
switch(config-track)# threshold percentage up 70 down 30
switch(config-track)# object 10
switch(config-track)# object 20
switch(config-track)# object 30
switch(config-track)#
```

This example shows how to configure a track list with an up weight threshold of 30 and a down threshold of 10:

```
switch# configure terminal
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
switch(config-track)# object 30
switch(config-track)#
```

In this example, the track list is up if object 10 and object 20 are up, and the track list goes to the down state if all three objects are down.

Related Commands

Command	Description
show track	Displays information about object tracking.
track ip route	Tracks an interface.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

V Commands

This chapter describes the Cisco NX-OS object tracking commands that begin with V.

Review Draft -- Cisco Confidential

vrf member

To add an interface to a virtual routing and forwarding (VRF) instance or to configure object tracking on a VRF instance, use the **vrf member** command. To remove the object tracking for this route, use the **no** form of this command.

vrf member *vrf-name*

no vrf member *vrf-name*

Syntax Description

vrf-name	VRF name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Interface configuration mode
Object tracking confiuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **vrf member** command in object tracking configuration mode to track objects in a nondefault VRF.

Examples

This example shows how to track an IP route in VRF Red:

```
switch(config)# track 1 ip route 10.10.10.0/8 reachability
switch(config-track)# vrf member Red
switch(config-track)#
```

This example shows how to add the Ethernet interface 1/5 to VRF RemoteOfficeVRF:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)#
```

Related Commands

Command	Description
show ip eigrp	Displays Enhanced Interior Gateway Routing Protocol (EIGRP) information.
show ip ospf interface	Displays Open Shortest Path First (OSPF) interface-related information.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

Command	Description
show track	Displays information about object tracking.
track ip route	Tracks an interface.

Review Draft -- Cisco Confidential

<I_Italic>Review Draft -- Cisco Confidential

PART 6

OSPF Commands

Review Draft -- Cisco Confidential

A Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with A.

Review Draft -- Cisco Confidential

area authentication (OSPF)

To enable authentication for an Open Shortest Path First (OSPF) area, use the **area authentication** command. To remove authentication for an area, use the **no** form of this command.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication** [**message-digest**]

Syntax Description

area-id	Identifier for the OSPF area where you want to enable authentication. Specify as either a positive integer value or an IP address.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the *area-id* argument.

Command Default

No authentication

Command Modes

OSPF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **area authentication** command to configure the authentication mode for the entire OSPF area.

The authentication type and authentication password must be the same for all OSPF devices in an area. Use the **ip ospf authentication-key** command in interface configuration mode to specify this password.

If you enable MD5 authentication with the **message-digest** keyword, you must configure a password with the **ip ospf message-digest-key** command in interface configuration mode.

This command requires the LAN Base Services license.

Examples

This example shows how to configure authentication for area 0 of OSPF routing process 201:

```
switch(config)# router ospf 201
switch(config-router)# area 0 authentication message-digest
switch(config-router)# interface ethernet 1/1
switch(config-if)# no switchport
switch(config-if)# ip ospf area 0
switch(config)-if# ip ospf message-digest-key 10 md5 0 adcdefgh
```

Related Commands

Review Draft -- Cisco Confidential

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
ip ospf authentication-key	Assigns a password for simple password authentication for OSPF.
ip ospf message-digest-key	Assigns a password for OSPF MD5 authentication.
show ip ospf interface	Displays OSPF interface-related information.

Review Draft -- Cisco Confidential

area default-cost (OSPF)

To specify a cost for the default summary route sent into an Open Shortest Path First (OSPF) stub or not-so-stubby area (NSSA), use the **area default-cost** command. To remove the assigned default route cost, use the **no** form of this command.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost** *cost*

Syntax Description

area-id	Identifier for the OSPF area where you want to configure the default cost. The area ID can be from 0 to 4294967295 or an IP address.
cost	Cost for the default summary route used for a stub or NSSA. The range is from 0 to 16777215.

Command Default

The summary route cost is based on the area border router that generated the summary route.

Command Modes

Route-configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **area default-cost** command on an Area Border Router (ABR) attached to a stub or NSSA to configure the metric for the summary default route generated by the ABR into the stub area.

This command requires the LAN Base Services license.

Examples

This example shows how to set a default cost of 20 to stub network 192.0.2.0:

```
switch(config)# router ospf 201
switch(config-router)# area 192.0.2.0 stub
switch(config-router)# area 192.0.2.0 default-cost 20
switch(config-router)#
```

Related Commands

Command	Description
area stub	Defines an area as a stub area.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

area filter-list (OSPF)

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the **area filter-list** command. To change or cancel the filter, use the **no** form of this command.

area *area-id* **filter-list route-map** *map-name* {**in** | **out**}

no area *area-id* **filter-list route-map** *map-name* {**in** | **out**}

Syntax Description

area-id	Identifier for the OSPF area where you want to configure filtering. Specify as either a positive integer value or an IP address.
route-map *map-name*	Specifies the name of a route map used as the filter policy. The *map-name* argument can be any alphanumeric string of up to 63 characters.
in	Filters networks sent to this area.
out	Filters networks sent from this area.

Command Default

None

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **area filter-list** command to filter Type 3 LSAs. If you apply the route map with the **in** keyword, the route map filters all Type 3 LSAs originated by the ABR to this area, including Type 3 LSAs that originated as a result of the **area range** command in another area.

If you apply the route map with the **out** keyword, the route map filters all Type 3 LSAs that are advertised by the ABR to all other areas including Type 3 LSAs that originate locally as a result of the **area range** command configured in this area.

Cisco Nexus 6000 implicitly denies any prefix that does not match an entry in the route map.

This command requires the LAN Base Services license.

Examples

This example shows how to filter prefixes that are sent from all other areas to area 1:

```
switch(config)# router ospf 202
switch(config-router)# area 1 filter-list route-map FilterExternal in
switch(config-router)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show ip ospf policy statistics area	Displays OSPF policy statistics for an area.

Review Draft -- Cisco Confidential

area nssa (OSPF)

To configure an area as an Open Shortest Path First (OSPF) not-so-stubby (NSSA) area, use the **area nssa** command. To remove the NSSA area, use the **no** form of this command.

area *area-id* **nssa** [**default-information-originate** [**route-map** *map-name*]] [**no-redistribution**] [**no-summary**] [**translate type7** [**always** | **never**] [**suppress-fa**]]

no area *area-id* **nssa** [**default-information-originate** [**route-map** *map-name*]] [**no-redistribution**] [**no-summary**] [**translate type7** [**always** | **never**] [**suppress-fa**]]

Syntax Description

area-id	Identifier for the OSPF NSSA area. The area ID can be from 0 to 4294967295 or an IP address.
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on NSSA area border router (ABR) or NSSA autonomous system border router (ASBR).
route-map *map-name*	(Optional) Filters the Type 7 default generation based on the route map. The *map-name* argument can be any alphanumeric string up to 63 characters.
no-redistribution	(Optional) Blocks redistributed link-state advertisements (LSAs) from entering this NSSA area. Use this keyword when the router is both an NSSA ASBR and an NSSA ABR and you want the **redistribute** command to import routes into the normal areas but not into the NSSA area.
no-summary	(Optional) Allows an area to be an NSSA area but not have summary routes injected into it.
translate type7	(Optional) Translates Type 7 LSAs to type 5 LSAs.
always	(Optional) Always translates LSAs.
never	(Optional) Never translates LSAs.
suppress-fa	(Optional) Suppresses the forwarding address in translated LSAs. The ABR uses 0.0.0.0 as the forwarding IPv4 address.

Command Default

None

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **area nssa** command to create an NSSA area in an OSPF autonomous system. We recommend that you understand the network topology before configuring forwarding address suppression for translated LSAs. Suboptimal routing might result because there might be better paths to reach the destination's forwarding address.

This command requires the LAN Base Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to configure area 1 as an NSSA area:

```
switch(config)# router ospf 10
switch(config-router)# area 1 nssa
switch(config-router)#
```

This example shows how to configure area 1 as an NSSA area and translate Type 7 LSAs from area 1 to Type 5 LSAs, but not place the Type 7 forwarding address into the Type 5 LSAs. (OSPF places 0.0.0.0 as the forwarding address in the Type 5 LSAs.)

```
switch(config)# router ospf 2
switch(config-router)# area 1 nssa translate type7 suppress-fa
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
redistribute	Redistributes routes learned from one routing protocol to another routing protocol domain.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

area range (OSPF)

To consolidate and summarize routes at an Open Shortest Path First (OSPF) area boundary, use the **area range** command. To disable this function, use the **no** form of this command.

area *area-id* **range** *ip-prefix* [**not-advertise**]

no area *area-id* **range** *ip-prefix* [**not-advertise**]

Syntax Description

area-id	Identifier for the OSPF area where you want to summarize routes. The area ID can be from 0 to 4294967295 or an IP address.
ip-prefix	IP prefix specified as IP address/subnet mask length (*A.B.C.D/LEN*).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Command Default

Disabled

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **area range** command only with Area Border Routers (ABRs) to consolidate or summarize routes for an area. The ABR advertises that a single summary route is advertised to other areas and condenses routing information at area boundaries.

You can configure OSPF to summarize addresses for many different sets of address ranges by configuring multiple **area range** commands.

This command requires the LAN Base Services license.

Examples

This example shows how to configure one summary route to be advertised by the ABR to other areas for all hosts on network 192.0.2.0:

```
switch(config-if)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.201 255.255.255.0
switch(config-if)# ip ospf area 201
switch(config-if)# exit
switch(config)# router ospf 12
switch(config-router)# area 0 range 192.0.2.0 255.255.0.0
switch(config-router)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

area stub (OSPF)

To define an area as an Open Shortest Path First (OSPF) stub area, use the **area stub** command. To remove the area, use the **no** form of this command.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub [no-summary]**

Syntax Description

area-id	Identifier for the OSPF stub area. The area ID can be from 0 to 4294967295 or an IP address.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Command Default

None

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **area stub** command to configure all devices attached to the stub area. Use the **area default-cost** command on an area border router (ABR) attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending Summary LSAs (Type 3 LSAs3) into the stub area.

This command requires the LAN Base Services license.

Examples

This example shows how to create stub area 33 in OSPF 209:

```
switch(config)# router ospf 201
switch(config-router)# area 33 stub
switch(config-router)#
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub area.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

area virtual-link (OSPF)

To define an Open Shortest Path First (OSPF) virtual link, use the **area virtual-link** command. To remove a virtual link, use the **no** form of this command.

area *area-id* **virtual-link** *router-id*

no area *area-id* **virtual-link** *router-id*

Syntax Description

area-id	Identifier for the OSPF area assigned to the transit area for the virtual link. The area ID can be from 0 to 4294967295 or an IP address.
router-id	Router ID associated with the virtual link neighbor. Specify as an IP address. The router ID appears in the **show ip ospf neighbors** display.

Command Default

None

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **area virtual-link** command to establish a virtual link from a remote area to the backbone area. In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

Use the **area virtual-link** command to enter the virtual link configuration mode where you can use the following commands:

- **authentication [key-chain | message-digest | null]**
- **authentication-key [0 | 3]** *key*
- **dead-interval** *seconds*
- **hello-interval** *seconds*
- **message-digest-key** *key-id* **md5** *key*
- **retransmit-interval** *seconds*
- **transmit-delay** *seconds*

See each command for syntax and usage details.

You must configure both sides of a virtual link with the same area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the **show ip ospf neighbors** command in any mode.

Note You cannot configure a virtual link on a not-so-stubby (NSSA) area.

Review Draft -- Cisco Confidential

This command requires the LAN Base Services license.

Examples

This example shows how to establish a virtual link between two devices, A, and B, with default values for all optional parameters:

```
Device A:
switch(config)# router ospf 1
switch(config-router)# router-id 192.0.2.2
switch(config-router)# area 1 virtual-link 192.0.2.1
switch(config-router-vlink)#

Device B:
switch(config# router ospf 209
switch(config-router)# router-id 192.0.2.1
switch(config-router)# area 1 virtual-link 192.0.2.2
switch(config-router-vlink)#
```

Related Commands

Command	Description
authentication (OSPF virtual link)	Enables authentication for an OSPF virtual link.
authentication-key (OSPF virtual link)	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
dead-interval (OSPF virtual link)	Configures the dead interval for an OSPF virtual link.
hello-interval (OSPF virtual link)	Configures the hello interval for an OSPF virtual link.
message-digest-key (virtual link)	Enables OSPF MD5 authentication in an OSPF virtual link.
retransmit-interval (OSPF virtual link)	Configures the retransmit interval for an OSPF virtual link.
show ip ospf neighbors	Displays OSPF neighbor information.
show ip ospf virtual-link	Displays OSPF virtual link information.
transmit-delay (OSPF virtual link)	Configures the transmit delay for an OSPF virtual link.

Review Draft -- Cisco Confidential

authentication (OSPF virtual link)

To specify the authentication type for an Open Shortest Path First (OSPF) virtual link, use the **authentication** command. To remove the authentication type for a virtual link, use the **no** form of this command.

authentication [**key-chain** *key-name* | **message-digest** | **null**]

no authentication

Syntax Description

key-chain *key-name*	(Optional) Specifies the key-chain to use. The *key-name* argument can be any alphanumeric string up to 63 characters.
message-digest	(Optional) Specifies to use message-digest authentication.
null	(Optional) Specifies no authentication is used. Disables authentication if configured for an area.

Command Default

Defaults to password authentication if you configure authentication with none of the optional keywords.

Command Modes

OSPF virtual link configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **authentication** command in virtual link configuration mode to configure the authentication method used on the virtual link. Use the **message-digest** keyword to configure MD5 message digest authentication and use the **message-digest-key** command to complete this authentication configuration. Use the **key-chain** keyword to configure password authentication using key chains and use the **key chain** command to complete this authentication configuration. Use the **authentication** command with no keywords to configure a password for the virtual link, and use the **authentication-key** command to complete this authentication configuration.

This command requires the LAN Base Services license.

Examples

This example shows how to enable message-digest authentication:

```
switch(config)# router ospf 22
switch(config-router)# area 99 virtual-link 192.0.2.12
switch(config-router-vlink)# authentication message-digest
switch(config-router-vlink)# message-digest key 4 md5 0 abcd
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
authentication-key (OSPF virtual link)	Assigns a password to be used by neighboring routers that are using the password authentication of OSPF.
key chain	Creates a key chain for managing authentication keys.
message-digest-key (OSPF virtual link)	Enables OSPF MD5 authentication.

Review Draft -- Cisco Confidential

authentication-key (OSPF virtual link)

To assign a password to be used by an Open Shortest Path First (OSPF) virtual link, use the **authentication-key** command. To remove a previously assigned OSPF password, use the **no** form of this command.

authentication-key [**0** | **3**] *password*

no authentication-key

Syntax Description

0	(Optional) Specifies an unencrypted authentication key.
3	(Optional) Specifies a 3DES encrypted authentication key.
password	Any continuous string of characters that can be entered from the keyboard up to 8 bytes.

Command Default

Unencrypted password

Command Modes

OSPF virtual link configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **authentication-key** command to configure the password for password authentication on an OSPF virtual link. All devices on the same virtual link must have the same password to be able to exchange OSPF information.

This command requires the LAN Base Services license.

Examples

This example shows how to enable the authentication key with the string yourpass:

```
switch(config)# router ospf 22
switch(config-router)# area 99 virtual-link 192.0.2.12
switch(config-router-vlink)# authentication
switch(config-router-vlink)# authentication-key yourpass
```

Related Commands

Command	Description
authentication (virtual link)	Enables authentication for an OSPF virtual link.

Review Draft -- Cisco Confidential

auto-cost (OSPF)

To control how Open Shortest Path First (OSPF) calculates default metrics for an interface, use the **auto-cost** command. To assign the default reference bandwidth of 40 Gb/s, use the **no** form of this command.

auto-cost reference-bandwidth *bandwidth* [**Gbps** | **Mbps**]

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth *bandwidth*	Sets the reference bandwidth used to calculate the default metrics for an interface. The range depends on whether you use the **Gbps** or **MBps** keywords.
Gbps	(Optional) Specifies the rate in Gbps (bandwidth). The range is from 1 to 4000; the default is 40.
Mbps	(Optional) Specifies the rate in Mbps (bandwidth). The range is from 1 to 4000000; the default is 40000.

Command Default

40 Gb/s. The bandwidth defaults to Gb/s if you do not specify the **Gpbs** or **Mbps** keyword.

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **auto-cost** command to set the reference bandwidth used by the OSPF cost-metric calculation.

The value set by the **ip ospf cost** command overrides the cost that results from the **auto-cost** command.

This command requires the LAN Base Services license.

Examples

This example shows how to set the reference bandwidth for all local interfaces in an OSPF instance:

```
switch(config)# router ospf 201
switch(config-router)# auto-cost reference-bandwidth 10
```

Related Commands

Command	Description
ip ospf cost	Explicitly specifies the cost of sending a packet on an interface.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with C.

Review Draft -- Cisco Confidential

clear ip ospf neighbor

To clear neighbor statistics and reset adjacencies for Open Shortest Path First (OSPF), use the **clear ip ospf neighbor** command.

clear ip ospf [*instance-tag*] **neighbor** {* | *neighbor-id* | *interface-type number* | **loopback** *number* | **port-channel** *number*} [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.
*	Clears all neighbors.
neighbor-id	Neighbor ID (as an IP address) of the neighbor to clear.
interface-type number	Interface from which to clear all neighbors.
loopback *number*	Clears all neighbors on a loopback interface.
port-channel *number*	Clears all neighbors on a port-channel interface.
vrf *vrf-name*	(Optional) Specifies the name of the OSPF virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **clear ip ospf neighbor** command to clear neighbor information from the **show ip ospf neighbor** command. Use the *instance-tag* argument to clear the neighbor details from one OSPF instance. If you do not use the *instance-tag* argument, Cisco Nexus 6000 clears the neighbor details from all OSPF instances. Use the **show ip ospf neighbor** command to find the neighbor ID.

This command requires the LAN Base Services license.

Examples

This example shows how to clear all OSPF neighbor details for neighbor 192.0.2.1 for instance tag 201:

```
switch# clear ip ospf 201 neighbor 192.0.2.1
```

This example shows how to clear all OSPF neighbor details for all OSPF instances:

```
switch# clear ip ospf neighbor *
```

This example shows how to clear all OSPF neighbor details for all neighbors on Ethernet interface 1/2 for OSPF instance 202:

Review Draft -- Cisco Confidential

```
switch# clear ip ospf 202 neighbor ethernet 1/2
```

Related Commands

Command	Description
show ip ospf neighbor	Displays details for OSPF neighbors including the neighbor ID.

Review Draft -- Cisco Confidential

clear ip ospf policy statistics

To clear policy statistics for Open Shortest Path First (OSPF), use the **clear ip ospf policy statistics** command.

clear ip ospf [*instance-tag*] **policy statistics** {**area** *area-id* **filter-list** {**in** | **out**} | **redistribute** {**bgp** *autonomous-system* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**}} [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.
area	Clears policy statistics for an area.
area-id	Area ID as an integer or IP address.
filter-list	Specifies the policy statistics for filtered prefixes between OSPF areas.
in	Filters prefixes sent into this OSPF area.
out	Filters prefixes sent from this OSPF area.
redistribution	Clears OSPF route redistribution statistics.
bgp *autonomous-system*	Specifies the autonomous system number for the Border Gateway Protocol. Specify the autonomous system number as x.y, where the range is from 1 to 65535 for both x and y, or as a single integer, where the range is from 1 to 65535.
direct	Specifies directly connected routes.
eigrp *id*	Specifies the autonomous system number for the Enhanced Interior Gateway Protocol. Specify the *id* argument as any case-sensitive, alphanumeric string.
ospf *id*	Specifies the Open Shortest Path First version 2 instance. Specify the *id* argument as any case-sensitive, alphanumeric string.
rip *id*	Specifies the Routing Information Protocol instance. Specify the *id* argument as any case-sensitive, alphanumeric string.
static	Specifies static routes.
vrf *vrf-name*	(Optional) Specifies the name of the OSPF virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Review Draft -- Cisco Confidential

Usage Guidelines

Use the **clear ip ospf statistics** command to learn the policy statistics shown in the **show ip ospf policy statistics** command. Use the *instance-tag* argument to clear the policy statistics from one OSPF instance. If you do not specify the instance tag, Cisco Nexus 6000 clears the policy statistics from all OSPF instances. Use the **show ip ospf policy statistics** command to to view the statistics that you are clearing.

This command requires the LAN Base Services license.

Examples

This example shows how to clear all OSPF policy statistics for area 99 inbound filtered routes for OSPF 201:

```
switch# clear ip ospf 201 policy statistics area 99 filter-list in
```

This example shows how to clear all OSPF policy statistics for all BGP redistributed routes for OSPF 202:

```
switch# clear ip ospf 202 policy statistics redistribute bgp
```

Related Commands

Command	Description
show ip ospf policy statistics	Displays details for OSPF policies.

Review Draft -- Cisco Confidential

clear ip ospf redistribution

To clear redistribution information for Open Shortest Path First (OSPF) , use the **clear ip ospf redistribution** command.

clear ip ospf redistribution [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is a case-sensitive, alphanumeric string of up to 32 characters.
all	(Optional) Specifies the “all” VRF instance.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear redistribution information:

```
switch# clear ip ospf redistribution
```

Related Commands

Command	Description
feature ospf	Enables the OSPF feature.

Review Draft -- Cisco Confidential

clear ip ospf statistics

To clear Open Shortest Path First (OSPF) event statistics, use the **clear ip ospf statistics** command.

clear ip ospf [*instance-tag*] **statistics** [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.
vrf *vrf-name*	(Optional) Specifies the name of the OSPF virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **clear ip ospf statistics** command to clear the event statistics from one or more OSPF instances. If you do not specify the *instance-tag* argument, Cisco Nexus 6000 clears statistics from all OSPF instances. Use the **show ip ospf statistics** command to to view the statistics that you are clearing.

This command requires the LAN Base Services license.

Examples

This example shows how to clear all OSPF event statistics:

```
switch# clear ip ospf statistics
```

Related Commands

Command	Description
show ip ospf statistics	Displays event statistics for OSPF.

Review Draft -- Cisco Confidential

clear ip ospf traffic

To clear Open Shortest Path First (OSPF) traffic statistics, use the **clear ip ospf traffic** command.

clear ip ospf [*instance-tag*] **traffic** [*interface*] [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.
interface	(Optional) Interface to clear traffic statistics for. Use the **?** option to see the interface options.
vrf *vrf-name*	(Optional) Specifies the name of the OSPF virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **clear ip ospf traffic** command to clear the traffic statistics from one or more OSPF instances. If you do not specify the *instance-tag* argument, Cisco Nexus 6000 clears traffic statistics from all OSPF instances. Use the **show ip ospf traffic statistics** command to view the statistics that you are clearing.

This command requires the LAN Base Services license.

Examples

This example shows how to clear OSPF traffic statistics for OSPF 100:

```
switch# clear ip ospf 100 traffic
```

Related Commands

Command	Description
show ip ospf traffic statistics	Displays OSPF traffic statistics.

Review Draft -- Cisco Confidential

clear ip traffic

To clear IP traffic information, use the **clear ip traffic** command.

clear ip traffic

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear the IP traffic information:

```
switch(config)# clear ip traffic
```

Related Commands

Command	Description
show ip traffic	Displays IP traffic information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

D Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with D.

Review Draft -- Cisco Confidential

dead-interval (OSPF virtual link)

To set the interval during which at least one hello packet must be received from a neighbor on an Open Shortest Path First (OSPF) virtual link before the router declares that neighbor as down, use the **dead interval** command. To restore the default, use the **no** form of this command.

dead-interval *seconds*

no dead-interval

Syntax Description

seconds	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or that neighbor is removed from the peer list and does not participate in routing. The range is from 1 to 65535. The value must be the same for all nodes on the virtual link.

Command Default

40 seconds

Command Modes

Virtual link configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **dead interval** command in virtual link configuration mode to configure the dead interval advertised in OSPF hello packets. This value must be the same for all networking devices on the virtual link. The default value for *seconds* is four times the interval set by the **hello-interval** command.

You can configure a shorter dead interval (*seconds*) to detect a down neighbor faster and improve convergence. A shorter dead interval may lead to virtual link instability by incorrectly declaring a slow neighbor as down.

Use the **show ip ospf virtual-links** command to verify the dead interval.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the OSPF dead interval to 20 seconds:

```
switch(config)# ospf 201
switch(config-router)# area 99 virtual-link 192.0.2.4
switch(config-router-vlink)# dead-interval 20
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
hello-interval (OSPF virtual link)	Specifies the interval between hello packets that Cisco NX-OS sends on the virtual link.
show ip ospf virtual-link	Displays OSPF virtual link information.

Review Draft -- Cisco Confidential

default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the **default-information originate** command. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**route-map** *map-name*]

no default-information originate [**always**] [**route-map** *map-name*]

Syntax Description

always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.
route-map *map-name*	(Optional) Specifies to advertise the default route if the route map is satisfied. The *map-name* argument can be any alphanumeric string up to 63 characters.

Command Default

Advertises the default route if the route is in the route table.

Command Modes

Address-family configuration mode

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **default-information originate** command to assign a default route for redistributed routes. Whenever you use the **redistribute** command to redistribute routes into an OSPF routing domain, Cisco NX-OS automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain.

Use the **route-map** keyword to filter redistributed routes so that Cisco Nexus 6000 generates a default route only for routes that pass the route map. Use the **always** keyword to generate the default route regardless of whether the default route is in the route table.

Note The **default-information originate** command ignores **match** statements in the optional route map.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the default route redistributed into the OSPF routing domain for the Enhanced Interior Gateway Protocol (EIGRP):

```
switch(config)# router ospf 109
switch(config-router)# redistribute eigrp 108 route-map EigrpPolicy
switch(config-router)# default-information originate always
```

Review Draft -- Cisco Confidential

```
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
redistribute (OSPF)	Redistributes routes from one routing domain into OSPF.
route-map	Defines a filter policy for routes.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

default-metric (OSPF)

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the **default-metric** command. To return to the default state, use the **no** form of this command.

default-metric *metric-value*

no default-metric *metric-value*

Syntax Description

metric-value	Default metric value appropriate for the specified routing protocol. The range is from 1 to 1677214.

Command Default

The metric for redistributed, connected, and static routes is set to 25.

Command Modes

Address-family configuration mode

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **default-metric** command with the **redistribute** command to configure the same metric value for all redistributed routes except static and directly connected routes. A default metric helps to redistribute routes with incompatible metrics. Whenever external route metrics do not convert to an OSPF metric, use a default metric to enable the redistribution to proceed.

Note The **default-metric** command does not apply to the redistribution of directly connected routes into OSPF. Use a route map to change the default metric for directly connected routes.

This command requires the LAN Base Services license.

Examples

This example shows how to configure OSPF to redistribute RIP and BGP and set the default metric to 10:

```
switch(config)# router ospf 201
switch(config-router)# default-metric 10
switch(config-router)# redistribute rip 109 route-map FilterRip
switch(config-router)# redistribute bgp 4 route-map FilterBgp
switch(config-router)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
redistribute (OSPF)	Redistributes routes from another routing domain into OSPF.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

distance (OSPF)

To define the Open Shortest Path First (OSPF) route administrative distance, use the **distance** command. To restore the default, use the **no** form of this command.

distance *distance*

no distance

Syntax Description

distance	Administrative distance for all routes local to this OSPF process. The range is from 1 to 255.

Command Default

110

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **distance** command to set a distance for an entire group of routes. Use the **distance** command when you configure multiple routing protocols, and you want to choose one set of routes over the other.

This command requires the LAN Base Services license.

Examples

This example shows how to set the distance to 200, making the route less reliable:

```
switch(config)# router ospf 1
switch(config-router)# distance 200
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with F.

Review Draft -- Cisco Confidential

feature ospf

To enable the Open Shortest Path First Protocol (OSPF), use the **feature ospf** command. To disable OSPF, use the **no** form of this command.

feature ospf

no feature ospf

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the OSPF feature before you can configure OSPF.

This command requires the LAN Base Services license.

Examples

This example shows how to enable the OSPF feature:

```
switch# configure terminal
switch(config)# feature ospf
switch(config)#
```

This example shows how to disable the OSPF feature:

```
switch# configure terminal
switch(config)# no feature ospf
switch(config)#
```

Related Commands

Command	Description
router ospf	Creates an OSPF instance.
show feature	Displays the status of features on a switch.
show ospf	Displays OSPF configuration information.

Review Draft -- Cisco Confidential

flush-routes (OSPF)

To flush routes on a restart for the Open Shortest Path First (OSPF) protocol, use the **flush-routes** command. To disable this feature, use the **no** form of this command.

flush-routes

no flush-routes

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command causes OSPF to unregister from the unicast RIB when OSPF shuts down. The unicast RIB removes all the routes associated with this OSPF instance. If you do not configure the **flush-routes** command, OSPF does not unregister and the OSPF routes will be stale. The OSPF routes are eventually removed from the unicast RIB after a timeout period.

This command requires the LAN Base Services license.

Examples

This example shows how to flush routes for an OSPF restart:

```
switch# configure terminal
switch(config)# router ospf 202
switch(config-router)# flush-routes
switch(config-router)#
```

Related Commands

Command	Description
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

H Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with H.

Review Draft -- Cisco Confidential

hello-interval (OSPF virtual link)

To specify the interval between hello packets that Cisco NX-OS sends on an Open Shortest Path First (OSPF) virtual link, use the **hello-interval** command. To return to the default setting, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description

seconds	Hello interval (in seconds). The value must be the same for all nodes on a specific virtual link. The range is from 1 to 65535.

Command Default

10 seconds

Command Modes

Virtual link configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **hello-interval** command in virtual link configuration mode to set the hello interval for OSPF across a virtual link. A shorter hello interval detects topological changes faster but causes more routing traffic. The hello interval must be the same for all devices on a virtual link.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the hello interval to 15 seconds:

```
switch(config)# router ospf 202
switch(config-router)# area 99 virtual-link 192.0.2.4
switch(config-router-vlink)# hello-interval 15
switch(config-router-vlink)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
dead-interval (virtual link)	Sets the time period to declare a neighbor as down if the local device receives no hello packets.
show ip ospf virtual-link	Displays OSPF virtual link information.

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with I.

Review Draft -- Cisco Confidential

ip ospf authentication

To specify the authentication type for an Open Shortest Path First (OSPF) interface, use the **ip ospf authentication** command. To remove the authentication type for an interface, use the **no** form of this command.

ip ospf authentication [**key-chain** *key-name* | **message-digest** | **null**]

no ip ospf authentication

Syntax Description

key-chain *key-name*	(Optional) Specifies a key chain to use for authentication. The *key-name* argument can be a maximum of 63 alphanumeric characters.
message-digest	(Optional) Specifies that message-digest authentication is used.
null	(Optional) Specifies that no authentication is used. Use this keyword to override any other authentication configured for an area.

Command Default

No authentication

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf authentication** command to configure the authentication mode for an OSPF interface. If you use this command with no keywords, use the **ip ospf authentication-key** command to configure the password. If you use the **message-digest** keyword, use the **ip ospf message-digest-key** command to configure the message-digest key for the interface.

The authentication that you configure on an interface overrides the authentication that you configure for the area.

This command requires the LAN Base Services license.

Examples

This example shows how to configure message-digest authentication:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf message-digest-key 33 md5 0 mypassword
switch(config-if)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the password authentication of OSPF.
ip ospf message-digest-key	Configures the OSPF MD5 message-digest key.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

ip ospf authentication-key

To assign a password for simple password authentication to be used by neighboring Open Shortest Path First (OSPF) routers, use the **ip ospf authentication-key** command. To remove a previously assigned OSPF password, use the **no** form of this command.

ip ospf authentication-key [**0** | **3** | **7**] *password*

no ip ospf authentication-key

Syntax Description

0	(Optional) Configures an unencrypted password.
3	(Optional) Configures a 3DES encrypted password string.
7	(Optional) Configures a Cisco type 7 encrypted password string.
password	Any continuous string of characters that can be entered from the keyboard up to 8 bytes.

Command Default

Unencrypted password

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf authentication-key** command to configure a password for simple password authentication. The password created by this command is used as a key that is inserted directly into the OSPF header when Cisco NX-OS originates routing protocol packets. You can assign a separate password to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

Note Cisco NX-OS uses this key when you enable authentication for an interface with the **ip ospf authentication** interface configuration command or if you configure the area for authentication with the **area authentication** command in router configuration mode.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an unencrypted authentication key with the string yourpass:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip ospf authentication-key yourpass
switch(config-if)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
area authentication	Specifies the authentication type for an OSPF area.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
ip ospf authentication	Specifies the authentication type for an interface.
show ip ospf interface	Displays OSPF information.

Review Draft -- Cisco Confidential

ip ospf cost

To specify the cost of sending a packet on an interface, use the **ip ospf cost** command. To reset the path cost to the default, use the **no** form of this command.

ip ospf cost *interface-cost*

no ip ospf cost *interface-cost*

Syntax Description

interface-cost	Unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Command Default

Calculates the cost based on the reference bandwidth divided by the configured interface bandwidth. You can configure the reference bandwidth or it defaults to 40 Gb/s.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf cost** command to configure the cost metric manually for each interface. This command overrides any settings for the reference bandwidth that you set using the **reference-bandwidth** command in router configuration mode.

If this command is not used, the link cost is calculated using the following formula:

link cost = reference bandwidth / interface bandwidth

This command requires the LAN Base Services license.

Examples

This example shows how to configure the interface cost value to 65:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf cost 65
switch(config-if)#
```

Related Commands

Command	Description
reference-bandwidth	Specifies the reference bandwidth that OSPF uses to calculate the link cost.

Review Draft -- Cisco Confidential

ip ospf dead-interval

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down, use the **ip ospf dead-interval** command. To restore the default, use the **no** form of this command.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Syntax Description

seconds	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or that neighbor adjacency is removed from the local router and does not participate in routing. The range is from 1 to 65535, and the default is 40. The value must be the same for all nodes on the network.

Command Default

The default for *seconds* is four times the interval set by the **ip ospf hello-interval** command.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf dead-interval** command to set the dead interval that Open Shortest Path First (OSPF) advertises in hello packets. This value must be the same for all networking devices on a specific network.

Configure a shorter dead interval to detect down neighbors faster and improve convergence. Very short dead intervals could cause routing instability.

Use the **show ip ospf interface** command to verify the dead interval and hello interval.

This command requires the LAN Base Services license.

Examples

This example shows how to set the OSPF dead interval to 20 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf dead-interval 20
switch(config-if)#
```

Related Commands

Command	Description
ip ospf hello-interval	Specifies the interval between hello packets that OSPF sends on the interface.
show ip ospf interface	Displays OSPF interface-related information.

Review Draft -- Cisco Confidential

ip ospf hello-interval

To specify the interval between hello packets that Open Shortest Path First (OSPF) sends on the interface, use the **ip ospf hello-interval** command. To return to the default, use the **no** form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Syntax Description

seconds	Interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.

Command Default

10 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf hello-interval** command to set the rate at which OSPF advertises hello packets. Shorter hello intervals allow OSPF to detect topological changes faster. This value must be the same for all routers and access servers on a specific network.

This command requires the LAN Base Services license.

Examples

This example shows how to set the interval between hello packets to 15 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf hello-interval 15
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
ip ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

ip ospf message-digest-key

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the **ip ospf message-digest-key** command. To remove an old MD5 key, use the **no** form of this command.

ip ospf message-digest-key *key-id* **md5** [**0** | **3** | **7**] *key*

no ip ospf message-digest-key *key-id*

Syntax Description

key-id	Identifier in the range from 1 to 255.
0	(Optional) Specifies an unencrypted password to generate the MD5 key.
3	(Optional) Specifies an encrypted 3DES password to generate the md5 key.
7	(Optional) Specifies a Cisco type 7 encrypted password to generate the MD5 key.
key	Alphanumeric password of up to 16 bytes.

Command Default

Unencrypted

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf message-digest-key** command when you configure the MD5 digest authentication mode. All neighbor routers must have the same *key* value on the network.

This command requires the LAN Base Services license.

Examples

This example shows how to set key 19 with the password 8ry4222:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf message-digest-key 19 md5 8ry4222
switch(config-if)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
ip ospf authentication	Specifies the authentication type for an interface.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

ip ospf mtu-ignore

To disable Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on received Database Descriptor (DBD) packets, use the **ip ospf mtu-ignore** command. To return to the default, use the **no** form of this command.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

OSPF MTU mismatch detection is enabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf mtu-ignore** command to disable MTU mismatch detection on an interface. By default, OSPF checks whether neighbors are using the same MTU on a common interface. If the receiving MTU is higher than the IP MTU configured on the incoming interface, OSPF does not establish adjacencies. Use the **ip ospf mtu-ignore** command to disable this check and allow adjacencies when the MTU value differs between OSPF neighbors.

This command requires the LAN Base Services license.

Examples

This example shows how to disable MTU mismatch detection on received DBD packets:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf mtu-ignore
switch(config-if)#
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing instances.
show ip ospf interface	Displays OSPF-related interface information.

Review Draft -- Cisco Confidential

ip ospf network

To configure the Open Shortest Path First (OSPF) network type to a type other than the default for an interface, use the **ip ospf network** command. To return to the default, use the **no** form of this command.

ip ospf network {**broadcast** | **point-to-point**}

no ip ospf network

Syntax Description

broadcast	Sets the network type as broadcast.
point-to-point	Sets the network type as point-to-point.

Command Default

Depends on the network type.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Command History

Usage Guidelines

The network type influences the behavior of the OSPF interface. An OSPF network type is usually broadcast, which uses OSPF multicasting capabilities. Under this network type, a designated router and backup designated router are elected. For point-to-point networks, there are only two neighbors and multicast is not required. For routers on an interface to become neighbors, the network type for all should match.

This command overrides the **medium** {**broadcast** | **p2p**} command in interface configuration mode.

This command requires the LAN Base Services license.

Examples

This example shows how to set an OSPF network as a broadcast network:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.33 255.255.255.0
switch(config-if)# ip ospf network broadcast
switch(config-if)#
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing instances.
show ip ospf interface	Displays OSPF-related interface information.

Review Draft -- Cisco Confidential

ip ospf passive-interface

To suppress Open Shortest Path First (OSPF) routing updates on an interface, use the **ip ospf passive-interface** command. To return to the default, use the **no** form of this command.

ip ospf passive-interface

no ip ospf passive-interface

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If an interface is configured as a passive interface, it does not participate in OSPF and does not establish adjacencies or send routing updates. However, the interface is announced as part of the routing network.

This command requires the LAN Base Services license.

Examples

This example shows how to set an interface as passive:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf passive-interface
switch(config-if)#
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing instances.
show ip ospf interface	Displays OSPF-related interface information.

Review Draft -- Cisco Confidential

ip ospf priority

To set the router priority for an Open Shortest Path First (OSPF) interface, use the **ip ospf priority** command. To return to the default, use the **no** form of this command.

ip ospf priority *number-value*

no ip ospf priority *number-value*

Syntax Description

number-value	Number that specifies the priority of the router. The range is from 0 to 255.

Command Default

Priority of 1

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf priority** command to set the router priority, which determines the designated router for this network. When two routers are attached to a network, both attempt to become the designated router. The router with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero cannot become the designated router or backup designated router.

Cisco Nexus 6000 uses this priority value when you configure OSPF for broadcast networks using the **neighbor** command in router configuration mode.

This command requires the LAN Base Services license.

Examples

This example shows how to set the router priority value to 4:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf priority 4
switch(config-if)#
```

Related Commands

Command	Description
ip ospf network	Configures the OSPF network type to a type other than the default for a given medium.

Review Draft -- Cisco Confidential

ip ospf retransmit-interval

To specify the time between Open Shortest Path First (OSPF) link-state advertisement (LSA) retransmissions for adjacencies that belongs to the interface, use the **ip ospf retransmit-interval** command. To return to the default, use the **no** form of this command.

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. The time must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

Command Default

5 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf retransmit-interval** command to set the time between LSA retransmissions. When a router sends an LSA to its neighbor, it keeps the LSA until it receives an acknowledgment message from the neighbor. If the router receives no acknowledgment within the retransmit interval, the local router resends the LSA.

This command requires the LAN Base Services license.

Examples

This example shows how to set the retransmit interval value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf retransmit-interval 8
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
ip ospf transmit-delay	Sets the estimated time to transmit an LSA to a neighbor.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

ip ospf shutdown

To shut down an Open Shortest Path First (OSPF) interface, use the **ip ospf shutdown** command. To return to the default, use the **no** form of this command.

ip ospf shutdown

no ip ospf shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf shutdown** command to shut down OSPF on this interface.

This command requires the LAN Base Services license.

Examples

This example shows how to shut down OSPF on an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf shutdown
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

ip ospf transmit-delay

To set the estimated time required to send an Open Shortest Path First (OSPF) link-state update packet on the interface, use the **ip ospf transmit-delay** command. To return to the default, use the **no** form of this command.

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 450 seconds, and the default is 1.

Command Default

1 second

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf transmit-delay** command to set the estimated time needed to send an LSA update packet. OSPF increments the LSA age time by the transmit delay amount before transmitting the LSA update. You should take into account the transmission and propagation delays for the interface when you set this value.

This command requires the LAN Base Services license.

Examples

This example shows how to set the transmit delay value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip ospf transmit-delay 8
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
ip ospf retransmit-interval	Sets the estimated time between LSAs transmitted from this interface.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

ip router ospf area

To specify the Open Shortest Path First (OSPF) instance and area for an interface, use the **ip router ospf area** command. To return to the default, use the **no** form of this command.

ip router ospf *instance-tag* **area** *area-id* [**secondaries none**]

no ip router ospf *instance-tag* **area** *area-id* [**secondaries none**]

Syntax Description

instance-tag	Instance tag. The *instance-tag* can be an alphanumeric string of 20 characters.
area-id	Identifier for the OSPF area where you want to enable authentication. The area ID can be either a positive integer value from 0 to 4294967295 or an IP address.
secondaries none	(Optional) Excludes secondary IP addresses.

Command Default

10 seconds

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip router ospf area** command to specify the area and OSPF instance for the interface.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an interface for OSPF:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router ospf Base area 33
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf interface	Displays OSPF interface-related information.

Review Draft -- Cisco Confidential

ip router ospf multi-area

To configure a multi-area adjacency on an Open Shortest Path First (OSPF) interface, use the **ip router ospf multi-area** command. To return to the default, use the **no** form of this command.

ip router ospf *instance-tag* **multi-area** *area-id*

no ip router ospf *instance-tag* **multi-area** *area-id*

Syntax Description

instance-tag	Instance tag. Specify as an case-sensative alphanumeric string up to 20 characters.
area-id	Identifier for the OSPF area where you want to add as another area to the primary interface. The area ID can be either a positive integer value from 0 to 4294967295 or an IP address.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, make sure that you enable OSPF on the switch.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a multi-area adjacency:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router ospf Base area 33
switch(config-if)# ip router ospf Base multi-area 99
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
feature ospf	Enables OSPF on the switch.
show ip ospf interface	Displays OSPF interface-related information.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

L Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with L.

Review Draft -- Cisco Confidential

log-adjacency-changes (OSPF)

To configure the router to send a syslog message when the state of an Open Shortest Path First (OSPF) neighbor changes, use the **log-adjacency-changes** command. To turn off this function, use the **no** form of this command.

log adjacency changes [**detail**]

Syntax Description

detail	(Optional) Provides all (DOWN, INIT, 2WAY, EXSTART, EXCHANGE, LOADING, FULL) adjacency state changes.

Command Default

The router sends a system message when the state of an OSPF neighbor changes.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **log-adjacency-changes** command to display high-level changes to the state of the OSPF neighbor relationship. This command is on by default but only reports the up/down (full/down) events if you do not use the **detail** keyword.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the router to send a system message when an OSPF neighbor state changes:

```
switch(config)# router ospf 209
switch(config-router)# log-adjacency-changes detail
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

M Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with M.

Review Draft -- Cisco Confidential

max-metric router-lsa (OSPF)

To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa** command. To disable the advertisement of a maximum metric, use the **no** form of this command.

max-metric router-lsa [**on-startup** [*seconds* | **wait-for bgp** *tag*]]

no max-metric router-lsa [**on-startup** [*seconds* | **wait-for bgp** *tag*]]

Syntax Description

on-startup	(Optional) Configures the router to advertise a maximum metric at startup.
seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.
wait-for bgp *tag*	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds. The *tag* name can be a maximum of 20 characters.

Command Default

Originates router link-state advertisements (LSAs) with normal link metrics.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **max-metric router-lsa** command to originate LSAs with a maximum metric (LSInfinity: 0xFFFF) through all nonstub links. This command allows Border Gateway Protocol (BGP) routing tables to converge without attracting transit traffic (if there are not alternate lower cost paths to the router). The router advertises accurate (normal) metrics after the configured or default timers expire or after BGP sends a notification that routing tables have converged.

Note Directly connected links in a stub network are not affected by the configuration of a maximum or infinite metric because the cost of a stub link is always set to the output interface cost.

You can use the **max-metric router-lsa** command in the following situations:

- Reloading a router. After a router is reloaded, Interior Gateway Protocols (IGPs) converge very quickly, and other routers may try to forward traffic through the newly reloaded router. If the router is still building BGP routing tables, the packets that are destined for other networks that the router has not learned through BGP may be dropped.

Review Draft -- Cisco Confidential

- Introducing a router into a network without routing traffic through it. You might want to connect a router to an OSPF network but not want real traffic to flow through the router if there are better alternate paths. If no alternate paths exist, then this router would still accept transit traffic.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a router that is running OSPF to advertise a maximum metric for 100 seconds:

```
switch(config)# router ospf 100
switch(config-router)# max-metric router-lsa on-startup 100
switch(config-router)#
```

This example shows how to configure a router to advertise a maximum metric until BGP routing tables converge or until the default timer expires (600 seconds):

```
switch(config)# router ospf 100
switch(config-router)# max-metric router-lsa on-startup wait-for bgp bgpTag
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

maximum-paths (OSPF)

To control the maximum number of parallel routes that Open Shortest Path First (OSPF) can support, use the **maximum-paths** command. To remove the **maximum-paths** command from the configuration file and restore the system to the default, use the **no** form of this command.

maximum-paths *maximum*

no maximum- paths

Syntax Description

maximum	Maximum number of parallel routes that OSPF can install in a routing table. The range is from 1 to 16 routes.

Command Default

8 paths

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **maximum-paths** command to allow OSPF to install multiple paths into the routing table for each prefix. Multiple paths are installed for both internal and external routes that are learned in the same autonomous system and that have an equal cost (according to the OSPF shortest path first algorithm).

This command requires the LAN Base Services license.

Examples

This example shows how to allow a maximum of 10 paths to a destination:

```
switch# configure terminal
switch(config)# router ospf 1
switch(config-router)# maximum-paths 10
switch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

message-digest-key (OSPF virtual link)

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication on a virtual link, use the **message-digest-key** command. To remove an old MD5 key, use the **no** form of this command.

message-digest-key *key-id* **md5** [**0** | **3**] *key*

no message-digest-key *key-id*

Syntax Description

key-id	Identifier in the range from 1 to 255.
0	(Optional) Specifies to use an unencrypted password to generate the md5 key.
3	(Optional) Specifies to use an encrypted 3DES password to generate the md5 key.
key	Alphanumeric password of up to 16 bytes.

Command Default

Unencrypted

Command Modes

Virtual link configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

When you configure the MD5 digest authentication mode, make sure that both interfaces on the virtual link have the same *key* value.

This command requires the LAN Base Services license.

Examples

This example shows how to set key 19 with the password 8ry4222:

```
switch(config-router)# area 22 virtual-link 192.0.2.2
switch(config-router-vlink)# message-digest-key 19 md5 8ry4222
switch(config-router-vlink)#
```

Related Commands

Command	Description
authentication (virtual-link)	Configures the authentication mode on a virtual link.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

P Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with P.

Review Draft -- Cisco Confidential

protocol shutdown (OSPF)

To shut down an Open Shortest Path First (OSPF) instance, use the **protocol shutdown** command. To disable this function, use the **no** form of this command.

protocol shutdown

no protocol shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The OSPF instance is enabled by default when configured.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **protocol shutdown** command to disable an instance of OSPF without removing the configuration.

This command requires the LAN Base Services license.

Examples

This example shows how to disable OSPF 209:

```
switch(config) router ospf 209
switch(config-router)# protocol shutdown
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing instances.

Review Draft -- Cisco Confidential

R Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with R.

Review Draft -- Cisco Confidential

redistribute (OSPF)

To inject routes from one routing domain into Open Shortest Path First (OSPF), use the **redistribute** command. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

redistribute {**bgp** *as-number* | **direct** | **eigrp** *id* | **ospf** *instance-tag* | **rip** *instance-tag* | **static**} [**route-map** *map-name*]

no redistribute {**bgp** *as-number* | **direct** | **eigrp** *as-number* | **ospf** *instance-tag* | **rip** *instance-tag* | **static**}

Syntax Description

bgp *as-number*	Distributes routes from Border Gateway Protocol (BGP). The *as-number* is a 2-byte or 4-byte autonomous system number. The range for 2-byte numbers is from 1 to 65535. The range for 4-byte numbers is from 1 to 4294967295.
direct	Distributes routes that are directly connected on an interface.
eigrp *id*	Distributes routes from EIGRP. The *id* argument can be any case-sensitive, alphanumeric string.
ospf *instance-tag*	Distributes routes from the OSPF protocol. This protocol is supported in the IPv4 address family. The *instance-tag* argument can be any case-sensitive, alphanumeric string of up to 20 characters.
rip *instance-tag*	Distributes routes from the RIP protocol. The *instance-tag* can be a maximum of 20 alphanumeric characters.
static	Redistributes IP static routes, including the default static route.
route-map *map-name*	(Optional) Specifies the identifier of a configured route map. Use a route map to filter which routes are redistributed into EIGRP. The *map-name* argument can be a maximum of 63 alphanumeric characters.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **redistribute** command to import routes from other routing protocols into OSPF. You should always use a route map to filter these routes to ensure that OSPF redistributes only the routes that you intend.

Review Draft -- Cisco Confidential

You must configure a default metric to redistribute routes from another protocol into OSPF. You can configure the default metric with the **default-metric** command or with the route map configured with the **redistribute** command.

Note If you redistribute static routes, Cisco NX-OS also redistributes the default static route.

This command requires the LAN Base Services license.

Examples

This example shows how to redistribute BGP routes into an OSPF autonomous system:

```
switch(config)# router ospf 209
switch(config-router)# redistribute bgp 64496
witch(config-router)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
default-metric (OSPF)	Sets the default metrics for routes redistributed into OSPF.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

redistribute maximum-prefix (OSPF)

To limit the number of routes redistributed into Open Shortest Path First (OSPF), use the **redistribute maximum-prefix** command. To return to the default setting, use the **no** form of this command.

redistribute maximum-prefix *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]]

no redistribute maximum-prefix *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]

Syntax Description

max	Maximum number of prefixes that OSPF will distribute. The range is from 0 to 65535.
threshold	(Optional) Percentage of maximum prefixes that triggers a warning message. The range is from 1 to 100. The default is 75 percent.
warning-only	(Optional) Logs a warning message when the maximum number of prefixes is exceeded.
widthdraw	(Optional) Withdraws all redistributed routes.
num-retries	(Optional) Number of times OSPF tries to retrieve the redistributed routes. The range is from 1 to 12. The default is 1.
timeout	(Optional) Time between retry attempts. The range is from 60 to 600 seconds. The default is 300.

Command Default

No limit

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **clear ip ospf redistribute** command if all routes are withdrawn.

This command requires the LAN Base Services license.

Examples

This example shows how to limit the number of redistributed routes into OSPF:

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

restart (OSPF)

To restart an Open Shortest Path First version 2 (OSPFv2) instance and remove all associated neighbors, use the **restart** command.

restart ospf *instance-tag*

Syntax Description

instance-tag	Internally used identification parameter for an OSPF routing instance. It is locally assigned and can be any word or positive integer. The *instance-tag* argument can be a maximum of 20 alphanumeric characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to restart the OSPFv2 instance and remove all neighbors:

```
switch(config)# restart ospf 12
switch(config)#
```

Related Commands

Command	Description
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

retransmit-interval (OSPF virtual link)

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies that belong to the virtual link, use the **retransmit-interval** command. To return to the default, use the **no** form of this command.

retransmit-interval *seconds*

retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. The time must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

Command Default

5 seconds

Command Modes

Virtual link configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use this command to set the LSA retransmission time. If a router receives no acknowledgment that an LSA was received, the router resends the LSA at the retransmission interval.

You should set this value larger for virtual links.

This command requires the LAN Base Services license.

Examples

This example shows how to set the retransmit interval value to 8 seconds:

```
switch(config)# router ospf 109
switch(config-router)# area 33 virtual-link 192.0.2.2
switch(config-router-vrf)# retransmit-interval 8
```

Related Commands

Command	Description
area virtual-link	Creates a virtual link in an OSPF area.

Review Draft -- Cisco Confidential

rfc1583compatibility

To configure RFC 1583 compatibility as the method used to calculate summary route costs, use the **rfc1583compatibility** command. To disable RFC 1583 compatibility, use the **no** form of this command.

rfc1583compatibility

no rfc1583compatibility

Syntax Description

This command has no arguments or keywords.

Command Default

RFC 1583 compatibility is disabled.

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To minimize the chance of routing loops, all Open Shortest Path First (OSPF) routers in an OSPF routing domain should have RFC compatibility set identically.

Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the **no rfc1583compatibility** command to enable the calculation method used per RFC 2328.

Examples

This example specifies that the router process is compatible with RFC 1583:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# router ospf 2
switch(config-router)# rfc1583compatibility
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing instances.

Review Draft -- Cisco Confidential

router ospf

To configure an Open Shortest Path First (OSPF) routing instance, use the **router ospf** command. To terminate an OSPF routing process, use the **no** form of this command.

router ospf *instance-tag*

no router ospf *instance-tag*

Syntax Description

instance-tag	Internally used identification parameter for an OSPF routing instance. It is locally assigned and can be any word or positive integer. The *instance-tag* argument can be a maximum of 20 alphanumeric characters.

Command Default

No OSPF routing instance is defined.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **router ospf** command to specify multiple OSPF routing instances in each router.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a basic OSPF instance:

```
switch(config)# router ospf 12
switch(config-router)#
```

This example shows how to delete an OSPF instance:

```
switch(config)# no router ospf 12
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays OSPF information.

Review Draft -- Cisco Confidential

router-id (OSPF)

To use a fixed router ID for an Open Shortest Path First (OSPF) instance, use the **router-id** command. To revert to the previous OSPF router ID behavior, use the **no** form of this command.

router-id *ip-address*

no router-id *ip-address*

Syntax Description

ip-address	Router ID in IP address format.

Command Default

If this command is not configured, OSPF chooses an IPv4 address as the router ID from one of its interfaces.

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **router-id** command to manually specify a unique 32-bit numeric value for the router ID. This action ensures that EIGRP can function regardless of the interface address configuration.

If this command is used on an OSPF instance that has neighbors, OSPF uses the new router ID at the next reload or at a restart of OSPF.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the router ID:

```
switch(config)# router ospf 12
switch(config-router)# router-id 192.0.2.1
```

Related Commands

Command	Description
router ospf	Configures the OSPF routing process.

Review Draft -- Cisco Confidential

S Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with S.

Review Draft -- Cisco Confidential

set forwarding-address

To set the Open Shortest Path First (OSPF) forwarding address for redistributed type-5 Link State Advertisements (LSAs), use the **set forwarding-address** command. To remove the address, use the **no** form of this command.

set forwarding-address

no forwarding-address

Syntax Description

This command has no arguments or keywords.

Command Default

No forwarding address is set as a default.

Command Modes

Route-map configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command is used by the OSPF to set the forwarding address for the redistributed type-5 LSAs. The value of the forwarding address specified by the autonomous system boundary router (ASBR) can be either 0.0.0.0 or nonzero. The 0.0.0.0 address indicates that the originating router (the ASBR) is the next hop.

If the ASBR redistributes routes and OSPF is not enabled on the next hop interface for those routes, the forwarding address is set to 0.0.0.0 .

All of the following conditions must be met to set the forwarding address field to a nonzero address:

- OSPF is enabled on the ASBR's next hop interface.
- ASBR’s next hop interface is non-passive under OSPF.
- ASBR’s next hop interface is not point-to-point.
- ASBR’s next hop interface is not point-to-multipoint.

For all other conditions, set the forwarding address to 0.0.0.0.

Examples

This example shows how to set the forwarding address:

```
switch(config)# route-map test1 10 permit
switch(config-route-map)# set forwarding-address
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Review Draft -- Cisco Confidential

shutdown (OSPF)

To stop an Open Shortest Path First (OSPF) instance without removing the configuration, use the **shutdown** command. To start a stopped OSPF instance, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

No process is stopped.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Entering the **shutdown** command stops a router process but does not remove any configuration parameters. The **shutdown** command is displayed in the running configuration file when enabled.

This command requires the LAN Base Services license.

Examples

This example shows how to stop an active OSPF instance:

```
switch(config)# router ospf firstcompany
switch(config-router)# shutdown
```

Related Commands

Command	Description
feature ospf	Enables OSPF on the router.
router ospf	Configures an OSPF instance.

Review Draft -- Cisco Confidential

summary-address (OSPF)

To create aggregate addresses for the Open Shortest Path First (OSPF) protocol, use the **summary-address** command. To return to the default, use the **no** form of this command.

summary-address *ip-prefix/length* [**not-advertise**] [**tag** *tag*]

no summary-address *ip-prefix/length* [**not-advertise**] [**tag** *tag*]

Syntax Description

ip-prefix/length	IP prefix designated for a range of addresses, including the prefix length. Specify *ip-prefix* as an IP address. Specify *length* as a number from 1 to 31.
not-advertise	(Optional) Suppresses routes that match the specified prefix/length pair.
tag *tag*	(Optional) Specifies the tag value that can be used as a match value for controlling redistribution using route maps. The range is from 1 to 65535.

Command Default

None

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **summary-address** command to create an aggregate address to replace a series of more-specific addresses. The metric used to advertise the summary is the smallest metric of all the more specific routes.

Use this command to help reduce the size of the routing table and allow an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the summary address 192.0.0.0 to include address 192.0.1.0, 192.0.2.0, 192.0.3.0, and so on. Only the address 192.0.0.0 is advertised in an external link-state advertisement.

```
switch(config)# router ospf 201
switch(config-router)# summary-address 192.0.0.0/16
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
redistribute (OSPF)	Redistributes external routing protocol routes into OSPF.
show ip ospf summary-address	Displays OSPF summary-address redistribution information.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) **show** commands.

Review Draft -- Cisco Confidential

show ip ospf

To display general information about Open Shortest Path First (OSPF) routing instances, use the **show ip ospf** command.

show ip ospf [*instance-tag*] [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. Use this tag to display OSPF information about a specific OSPF instance. The *instance-tag* argument can be any alphanumeric string of 20 characters.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf** command to display information about one or more OSPF instances.

This command requires the LAN Base Services license.

Examples

This example shows how to display information all about OSPF instances:

```
switch# show ip ospf
Routing Process 201 with ID 192.0.2.1 VRF default
 Stateful High Availability enabled
 Graceful-restart is configured
   Grace period: 60 state: Inactive
   Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an autonomous system boundary
 Redistributing External Routes from
   bgp-1
   Maximum limit: 1000 (warning-only)
   Threshold: message 750
   Current count: 0
 Administrative distance 110
 Reference Bandwidth is 40000 Mbps
 Initial SPF schedule delay 3000.000 msecs,
   minimum inter SPF delay of 2000.000 msecs,
   maximum inter SPF delay of 4000.000 msecs
```

Review Draft -- Cisco Confidential

```
 Initial LSA generation delay 3000.000 msecs,
   minimum inter LSA delay of 6000.000 msecs,
   maximum inter LSA delay of 6000.000 msecs
 Minimum LSA arrival 2000.000 msec
 Maximum paths to destination 3
 Originating router LSA with maximum metric
   Condition: Always
 Number of external LSAs 0, checksum sum 0
 Number of opaque AS LSAs 0, checksum sum 0
 Number of areas is 3, 3 normal, 0 stub, 0 nssa
 Number of active areas is 0, 0 normal, 0 stub, 0 nssa
   Area BACKBONE(0.0.0.0) (Inactive)
        Area has existed for 00:22:49
        Interfaces in this area: 1 Active interfaces: 0
        Passive interfaces: 0  Loopback interfaces: 0
        No authentication available
        SPF calculation has run 3 times
         Last SPF ran for 0.000036s
        Area ranges are
        Number of LSAs: 0, checksum sum 0
   Area (0.0.0.10) (Inactive)
        Area has existed for 00:41:30
        Interfaces in this area: 0 Active interfaces: 0
        Passive interfaces: 0  Loopback interfaces: 0
        Summarization is disabled
        Simple password authentication
        SPF calculation has run 8 times
         Last SPF ran for 0.000150s
        Area ranges are
          10.3.0.0/16 Passive (Num nets: 0) Advertise
        Area-filter in 'FilterLSAs'
        Number of LSAs: 0, checksum sum 0
   Area (0.0.0.15) (Inactive)
        Area has existed for 00:49:30
        Interfaces in this area: 1 Active interfaces: 0
        Passive interfaces: 1  Loopback interfaces: 0
        No authentication available
        SPF calculation has run 8 times
         Last SPF ran for 0.000021s
        Area ranges are
        Number of LSAs: 0, checksum sum 0
switch#
```

This example shows how to display information about one specific OSPF instance:

```
switch# show ip ospf 201
Routing Process 201 with ID 192.0.2.1 VRF default
 Stateful High Availability enabled
 Graceful-restart is configured
   Grace period: 60 state: Inactive
   Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Administrative distance 110
 Reference Bandwidth is 40000 Mbps
 Initial SPF schedule delay 200.000 msecs,
   minimum inter SPF delay of 1000.000 msecs,
   maximum inter SPF delay of 5000.000 msecs
 Initial LSA generation delay 0.000 msecs,
   minimum inter LSA delay of 5000.000 msecs,
   maximum inter LSA delay of 5000.000 msecs
 Minimum LSA arrival 1000.000 msec
 Maximum paths to destination 3
 Number of external LSAs 0, checksum sum 0
```

Review Draft -- Cisco Confidential

```
 Number of opaque AS LSAs 0, checksum sum 0
 Number of areas is 2, 1 normal, 1 stub, 0 nssa
 Number of active areas is 0, 0 normal, 0 stub, 0 nssa
   Area (0.0.0.10) (Inactive)
        Area has existed for 00:12:18
        Interfaces in this area: 0 Active interfaces: 0
        Passive interfaces: 0  Loopback interfaces: 0
        This area is a STUB area
        Generates stub default route with cost 25
        Simple password authentication
        SPF calculation has run 1 times
         Last SPF ran for 0.000122s
        Area ranges are
        Area-filter in 'FilterLSAs'
        Number of LSAs: 0, checksum sum 0
   Area (0.0.0.15) (Inactive)
        Area has existed for 00:20:18
        Interfaces in this area: 1 Active interfaces: 0
        Passive interfaces: 1  Loopback interfaces: 0
        No authentication available
        SPF calculation has run 1 times
         Last SPF ran for 0.000020s
        Area ranges are
        Number of LSAs: 0, checksum sum 0
switch#
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip ospf Field Descriptions

Field	Description
Routing Process...	OSPF instance tag and OSPF router ID.
Stateful High Availability	Status of stateful restart capability.
Supports...	Number of types of service supported (Type 0 only).
Administrative distance	Administrative distance for the OSPFv2 instance.
Reference Bandwidth	Bandwidth used for cost calculation.
Initial SPF schedule delay	Delay time of SPF calculations.
Initial LSA generation delay	Delay time of LSA generations.
Minimum LSA arrival	Minimum interval between link-state advertisements.
Maximum paths to destination	Maximum paths to the neighbor.
Number of...	Number and type of link-state advertisements that have been received.
Number of areas is...	Number and type of areas configured for the router.
Number of active areas is	Number and type of active areas configured on the router.

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf border-routers

To display the Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ip ospf border-routers** command.

show ip ospf [*instance-tag*] **border-routers** [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. Use this tag to display OSPF information about a specific OSPF instance. The *instance-tag* argument can be a maximum of 20 alphanumeric characters.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf border-routers** command to display information on ABRs. and ASBRs.

This command requires the LAN Base Services license.

Examples

This example shows how to display information about border routers:

```
switch# show ip ospf border-routers
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf database

To display the Open Shortest Path First (OSPF) database for a specific router, use the **show ip ospf database** command.

show ip ospf [*instance-tag*] **database** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database asbr-summary** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database database-summary** [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database external** [**ext_tag** *value*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database network** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database nssa-external** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database opaque-area** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database opaque-as** [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database opaque-link** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database router** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

show ip ospf [*instance-tag*] **database summary** [*area-id*] [*link-state-id*] [**adv-router** *ip-address* | **self-originated**] [**detail**] [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. The name can be a maximum of 20 alphanumeric characters.
area-id	(Optional) Area number used to define the particular area. Specify as either an IP address or a number from 0 to 4294967295.
link-state-id	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's link-state type. Specify in the form of an IP address.
adv-router *ip-address*	(Optional) Displays all the link-state advertisements (LSAs) of the specified router.
self-originate	(Optional) Displays self-originated LSAs (from the local router).
asbr-summary	(Optional) Displays information about the autonomous system boundary router summary LSAs.
database-summary	(Optional) Displays each type of LSA for each area in the database, and the total number of LSAs.

Review Draft -- Cisco Confidential

external	(Optional) Displays information about the external LSAs.
ext_tag *value*	(Optional) Displays information based on an external tag. The range is from 1 to 4294967295.
network	(Optional) Displays information about the network LSAs.
nssa-external	(Optional) Displays information about the not-so-stubby area (NSSA) external LSAs.
opaque-area	(Optional) Displays information about the opaque area LSAs.
opaque-as	(Optional) Displays information about the opaque AS LSAs.
opaque-link	(Optional) Displays information about the opaque link-local LSAs.
router	(Optional) Displays information about the router LSAs.
summary	(Optional) Displays information about the summary LSAs.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf database** command to display information about different OSPF LSAs.

When the link state advertisement is describing a network, the *link-state-id* argument can take one of two forms:

- The network’s IP address (such as Type 3 summary link advertisements and autonomous system external link advertisements).
- A derived address obtained from the link state ID. (Note that masking a network links advertisement’s link state ID with the network’s subnet mask yields the network’s IP address.)
- When the link state advertisement is describing a router, the link state ID is always the described router’s OSPF router ID.
- When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).

This command requires the LAN Base Services license.

Examples

This example shows how to display the OSPF database:

```
switch# show ip ospf database
```

This example shows how to display a summary of autonomous system border routers:

Review Draft -- Cisco Confidential

```
switch# show ip ospf database asbr-summary
```

This example shows how to display information about external links:

```
switch# show ip ospf database external
```

This example shows how to display a summary of the OSPF database:

```
switch# show ip ospf database database-summary
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **show ip ospf interface** command.

show ip ospf interface [*instance-tag*] [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*}] [**brief**] [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. The name can be a maximum of 20 alphanumeric characetrs.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses, masks, and areas on the router.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf interface** command to display the OSPF status for the interface.

This command requires the LAN Base Services license.

Examples

This example shows how to display OSPF information for Ethernet interface 1/5:

```
switch# show ip ospf interface ethernet 1/5
Ethernet1/5 is up, line protocol is down
    IP address 192.0.2.1, Process ID 201 VRF RemoteOfficeVRF, area 0.0.0.10
    Enabled by interface configuration
    State DOWN, Network type BROADCAST, cost 4
    Index 1, Transmit delay 1 sec, Router Priority 1
    No designated router on this network
    No backup designated router on this network
```

Review Draft -- Cisco Confidential

```
    0 Neighbors, flooding to 0, adjacent with 0
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
    No authentication
    Number of opaque link LSAs: 0, checksum sum 0
switch#
```

Table 2 describes the significant fields shown in the display.

Table 2 show ip ospf interface Field Descriptions

Field	Description
Ethernet	Status of physical link and operational status of protocol.
IP Address	Interface IP address, subnet mask, and area address.
VRF	Virtual routing and forwarding (VRF) instance.
Transmit Delay	Transmit delay, interface state, and router priority.
designated router	Designated router ID and interface IP address.
backup designated router	Backup designated router ID and interface IP address.
Timer intervals	Configuration information of timer intervals.
Hello	Number of seconds until next hello packet is sent out this interface.

This example shows how to display OSPF information for all VRFs:

```
switch# show ip ospf interface vrf all
VL1-0.0.0.10-10.1.2.3 is down, line protocol is down
    IP address 0.0.0.0, Process ID 201 VRF default, area 0.0.0.0
    State DOWN, Network type P2P, cost 65535
    Index 2, Transmit delay 2 sec
    0 Neighbors, flooding to 0, adjacent with 0
    Timer intervals: Hello 25, Dead 50, Wait 50, Retransmit 50
    Message-digest authentication, using key id 21
    Number of opaque link LSAs: 0, checksum sum 0

switch#
```

This example shows how to display OSPF information in a brief format:

```
switch# show ip ospf interface brief
 OSPF Process ID 201 VRF default
 Total number of interface: 1
 Interface               ID     Area            Cost   State    Neighbors Status
 VL1                     2      0.0.0.0         65535  DOWN     0         down

switch#
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf lsa-content-changed-list

To display a list of all link-state advertisements (LSAs) with changed content, use the **show ip ospf lsa-content-changed-list** command.

show ip ospf lsa-content-changed-list *neighbor-id* {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*}

Syntax Description

neighbor id	Router ID for the neighbor in the format *A.B.C.D*.
ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display a list of LSAs that changed for Ethernet 2/1:

```
switch# show ip ospf lsa-content-changed-list 192.0.2.2 ethernet 2/1
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf neighbors

To display Open Shortest Path First (OSPF)-neighbor information on a per-interface basis, use the **show ip ospf neighbors** command.

show ip ospf [*instance-tag*] **neighbors** [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*}] [*neighbor-id*] [**detail**] [**summary**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. Specify as an alphanumeric string of 20 characters.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
neighbor-id	(Optional) Router ID of the neighbor. Specify as an IP address.
detail	(Optional) Displays all neighbors given in detail (lists all neighbors).
summary	(Optional) Displays a summary of the neighbors.
vrf	(Optional) Specifies a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRF entries.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf neighbors** command to display information about all or some of the neighbors for this OSPF instance.

This command requires the LAN Base Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to display the summary information about the neighbor that matches the neighbor ID:

```
switch# show ip ospf neighbors 10.199.199.137
```

This example shows how to display the neighbors that match the neighbor ID on an interface:

```
switch# show ip ospf neighbors ethernet 2/1 10.199.199.137
```

This example shows how to display detailed information about OSPF neighbors:

```
switch# show ip ospf neighbors detail
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf policy statistics area

To display Open Shortest Path First (OSPF) policy statistics for an area, use the **show ip ospf policy statistics area** command.

show ip ospf [*instance-tag*] **policy statistics area** *area-id* **filter-list** {**in** | **out**} [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
area *area-id*	Specifies the area number used to define the particular area. The area ID can be an IP address or a number from 0 to 4294967295.
filter-list	Filters prefixes between OSPF areas.
in	Displays policy statistics for incoming routes.
out	Displays policy statistics for outgoing routes.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default”, “management”, and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf policy statistics area** command to display information about the filter lists applied to an area.

This command requires the LAN Base Services license.

Examples

This example shows how to display policy statistics for OSPF:

```
switch# show ip ospf policy statistics area 201 filter-list in
```

Related Commands

Command	Description
area filter-list (OSPF)	Filters incoming or outgoing Network Summary (type 3) link-state advertisements (LSAs) on an Area Border Router (ABR).

Review Draft -- Cisco Confidential

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf policy statistics redistribute

To display Open Shortest Path First (OSPF) policy statistics, use the **show ip ospf policy statistics redistribute** command.

show ip ospf [*instance-tag*] **policy statistics redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
bgp	Displays policy statistics for the Border Gateway Protocol (BGP).
direct	Displays policy statistics for directly connected routes only.
eigrp	Displays policy statistics for the Enhanced Interior Gateway Routing Protocol (EIGRP).
ospf	Displays policy statistics for OSPF.
rip	Displays policy statistics for the Routing Information Protocol (RIP).
static	Displays policy statistics for IP static routes.
id	For the **bgp** keyword, an autonomous system number. The range for 2-byte numbers is from 1 to 65535. For the **eigrp** keyword, an autonomous system number. The range is from 1 to 65535. For the **ospf** and **rip** keywords, an instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default”, “management”, and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf policy statistics redistribute** command to display redistribution statistics.

This command requires the LAN Base Services license.

Examples

This example shows how to display policy statistics for redistributed routes:

Review Draft -- Cisco Confidential

```
switch# show ip ospf policy statistics redistribute
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ip ospf request-list** command.

show ip ospf request-list *neighbor-id* {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*}

Syntax Description

neighbor-id	Router ID of the neighbor. Specify as an IP address.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf request-list** command to troubleshoot Open Shortest Path First (OSPF) routing operations.

This command requires the LAN Base Services license.

Examples

This example shows how to display a list of all LSAs requested by a router:

```
switch# show ip ospf request-list 40.40.40 ethernet 2/1
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be resent to neighbors, use the **show ip ospf retransmission-list** command.

show ip ospf retransmission-list *neighbor-id* {**ethernet** *slot*/*port* | **loopback** *if_number* | **port-channel** *number*}

Syntax Description

neighbor-id	Router ID of the neighbor. Specify as an IP address.
ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf retransmission-list** command to troubleshoot Open Shortest Path First (OSPF) routing operations.

This command requires the LAN Base Services license.

Examples

This example shows how to display all LSAs waiting to be resent to neighbors:

```
switch# show ip ospf retransmission-list 192.0.2.11 ethernet 2/1
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf route

To display the Open Shortest Path First (OSPF) topology table, use the **show ip ospf routes** command.

show ip ospf [*instance-tag*] **routes** [*prefix/length* | **summary**} [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. Specify as an alphanumeric string of 20 characters.
prefix/length	(Optional) IP prefix, which limits output to a specific route. Indicate the length as a slash (/) and number from 1 to 31. For example, /8 indicates that the first eight bits in the IP prefix are network bits.
summary	(Optional) Displays a summary of all routes.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default”, “management”, and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ospf routes** command to display the OSPF private routing table (which contains only routes that are calculated by OSPF). If something is wrong with a route in the routing information base (RIB), then you should check the OSPF copy of the route to determine if it matches the RIB contents. If it does not match, a synchronization problem exists between OSPF and the RIB.

This command requires the LAN Base Services license.

Examples

This example shows how to display OSPF routes:

```
switch# show ip ospf route
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf statistics

To display Open Shortest Path First (OSPF) shortest path first (SPF) calculation statistics, use the **show ip ospf statistics** command.

show ip ospf [*instance-tag*] **statistics** [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. Specify as an alphanumeric string up to 20 characters.
vrf *vrf-name*	(Optional) Name of the VRF. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default”, “management”, and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf statistics** command to display information about link-state advertisements (LSAs). This information can be useful for both OSPF network maintenance and troubleshooting. For example, we recommend that you use the **show ip ospf statistics** command as the first troubleshooting step for LSA flapping.

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the SPF calculations:

```
switch# show ip ospf statistics
 OSPF Process ID 201 VRF default, Event statistics (cleared 00:10:45 ago)
  Router ID changes: 1
  DR elections: 0
  Older LSAs received: 0
  Neighbor state changes: 0
  Neighbor dead postponed: 0
  Neighbor dead interval expirations: 0
  Neighbor bad lsreqs: 0
  Neighbor sequence number mismatches: 0
  SPF computations:  2 full, 0 summary, 0 external

        LSA Type Generated Refreshed   Flushed  Aged out
          Router         0         0         0         0
         Network         0         0         0         0
     Summary Net         0         0         0         0
    Summary ASBR         0         0         0         0
     AS External         0         0         0         0
```

Review Draft -- Cisco Confidential

```
    Opaque Link          0          0          0          0
    Opaque Area          0          0          0          0
      Opaque AS          0          0          0          0

  Following counters can not be reset:

  LSA deletions: 0 pending, 0 hwm, 0 deleted, 0 revived, 0 runs
  Hello queue: 0/200, hwm 0, drops 0
  Flood queue: 0/350, hwm 0, drops 0
  LSDB additions failed: 0

        Buffers:    in use       hwm permanent     alloc      free
     128 bytes           0         0         0         0         0
     512 bytes           0         0         0         0         0
    1520 bytes           0         0         0         0         0
    4500 bytes           0         0         0         0         0
          huge           0         0         0         0         0

switch#
```

Table 3 describes the significant fields shown in the display.

Table 3 show ip ospf statistics Field Descriptions

Field	Description
OSPF process	Unique value assigned to the OSPF instance in the configuration.
VRF	Virtual routing and forwarding (VRF) for this OSPF instance.
DR elections	Number of times that a new designated router was elected.
Neighbor...	Details about neighbors.
LSA Type	Number of each type of LSA sent.
Hello queue	Queue of hello packets to be processed: • current number in queue/maximum number allowed in queue. • hwm—high water mark. The maximum number of packets ever stored in the queue. • drops—The number of packets dropped because the queue was full.
Flood queue	Queue of flood packets to be processed.
Buffers	Chunks of memory used to store packets.

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf summary-address

To display a list of all summary address redistribution information configured in an Open Shortest Path First (OSPF) instance, use the **show ip ospf summary-address** command.

show ip ospf [*instance-tag*] **summary-address** [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. The name can be a maximum of 20 alphanumeric characters.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default”, “management”, and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about summary addresses:

```
switch# show ip ospf summary-address
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip ospf traffic

To display Open Shortest Path First (OSPF) traffic statistics, use the **show ip ospf traffic** command.

show ip ospf [*instance-tag*] **traffic** [**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*] [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Name of the OSPF instance. The name can be a maximum of 20 alphanumeric characters.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default”, “management”, and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf traffic** command to display traffic statistics for one or more OSPF instances.

This command requires the LAN Base Services license.

Examples

This example shows how to display OSPF traffic statistics for interface 1/5:

```
switch# show ip ospf traffic ethernet 1/5
 OSPF Process ID 201 VRF RemoteOfficeVRF, Packet Counters (cleared 00:26:04 ago)
 Interface Ethernet1/5, Area 0.0.0.0
  Total: 0 in, 0 out
  LSU transmissions: first 0, rxmit 0, for req 0, nbr xmit 0
  Flooding packets output throttled (IP/tokens): 0 (0/0)
  Ignored LSAs: 0, LSAs dropped during SPF: 0
  LSAs dropped during graceful restart: 0
  Errors: drops in        0, drops out       0, errors in       0,
          errors out      0, hellos in       0, dbds in         0,
          lsreq in        0, lsu in          0, lsacks in       0,
```

Review Draft -- Cisco Confidential

```
          unknown in      0, unknown out     0, no ospf         0,
          bad version     0, bad crc         0, dup rid         0,
          dup src         0, invalid src     0, invalid dst     0,
          no nbr          0, passive         0, wrong area      0,
          pkt length      0, nbr changed rid/ip addr            0
          bad auth        0

           hellos       dbds     lsreqs       lsus       acks
   In:          0          0          0          0          0
  Out:          0          0          0          0          0

switch#
```

Table 4 describes the significant fields shown in the display.

Table 4 show ospf traffic Field Descriptions

Field	Description
OSPF Process	OSPF instance tag for these traffic statistics.
VRF	Virtual routing and forwarding (VRF) for this OSPF instance.
Interface ...	Interface information.
Errors	
drops	Number of packets dropped.
bad version	Number of packets received with bad version.
dup src	Number of packets with a duplicate source address.
no nbr	Number of packets from a router that is not a full neighbor.
nbr changed rid/ip addr	Number of packets with router-id/ip address pair not matching our neighbor's values.
lsreq	Number of packets of type LSREQ (LSA required).
acks	Number of packets of type LSACK (LSA acknowledged).

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPF traffic statistics.
show running-config ospf	Displays the OSPF running configuration information.

Review Draft -- Cisco Confidential

show ip ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **show ip ospf virtual-links** command.

show ip ospf [*instance-tag*] **virtual-links** [**brief**] [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) Instance tag. The name can be a maximum of 20 alphanumeric characters.
brief	(Optional) Displays a summary of the configured virtual links.
vrf *vrf-name*	(Optional) Name of the OSPF VRF. The *vrf-name* argument can be specified as an arbitrary string of 32 alphanumeric characters. The strings “default”, “management”, and “all” are reserved *vrf-names*.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip ospf virtual-links** command to display information about configured virtual links.

This command requires the LAN Base Services license.

Examples

This example shows how to display information about virtual links:

```
switch# show ip ospf virtual-links
 Virtual link VL1 to router 10.1.2.3 is down
    Transit area 0.0.0.10, via interface (null), remote addr 0.0.0.0
    IP address 0.0.0.0, Process ID 201 VRF default, area 0.0.0.0
    State DOWN, Network type P2P, cost 65535
    Index 2, Transmit delay 2 sec
    0 Neighbors, flooding to 0, adjacent with 0
    Timer intervals: Hello 25, Dead 50, Wait 50, Retransmit 50
    Message-digest authentication, using key id 21
    Number of opaque link LSAs: 0, checksum sum 0
    Adjacency Information

switch#
```

Table 5 describes the significant fields shown in the display.

Review Draft -- Cisco Confidential

Table 5 show ip ospf virtual-links Field Descriptions

Field	Description
Virtual Link	OSPF neighbor and whether the link to that neighbor is up or down.
VRF	Virtual routing and forwarding (VRF) for this OSPF instance.
Transit area...	Transit area through which the virtual link is formed.
via interface...	Interface through which the virtual link is formed.
cost	Cost of reaching the OSPF neighbor through the virtual link.
Transmit delay	Transmit delay (in seconds) on the virtual link.
Timer intervals...	Various timer intervals configured for the link.
Hello	Time when the next hello is expected from the neighbor.

This example shows how to display information about virtual links in brief format:

```
switch# show ip ospf virtual-links brief
 OSPF Process ID 201 VRF default
 Total number of vlinks: 1
 Remote Router    ID     Transit Area    Cost    Status
 10.1.2.3         1      0.0.0.10        65535   down

switch#
```

Related Commands

Command	Description
show running-config ospf	Displays the OSPF running configuration.

Review Draft -- Cisco Confidential

show ip traffic

To display IP traffic information, use the **show ip traffic** command.

show ip traffic

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the IP traffic information:

```
switch(config)# show ip traffic

IP Software Processed Traffic Statistics
----------------------------------------
Transmission and reception:
  Packets received: 103598, sent: 32093, consumed: 2,
  Forwarded, unicast: 0, multicast: 0, Label: 0
Opts:
  end: 0, nop: 0, basic security: 0, loose source route: 0
  timestamp: 0, record route: 0
  strict source route: 0, alert: 0,
  other: 0
Errors:
  Bad checksum: 0, packet too small: 0, bad version: 0,
  Bad header length: 0, bad packet length: 0, bad destination: 0,
  Bad ttl: 0, could not forward: 990, no buffer dropped: 0,
  Bad encapsulation: 2, no route: 0, non-existent protocol: 0
  Stateful Restart Recovery: 0
  MBUF pull up fail: 0
Fragmentation/reassembly:
  Fragments received: 0, fragments sent: 0, fragments created: 0,
  Fragments dropped: 0, packets with DF: 0, packets reassembled: 0,
  Fragments timed out: 0

ICMP Software Processed Traffic Statistics
------------------------------------------
Transmission:
  Redirect: 2, unreachable: 0, echo request: 0, echo reply: 0,
  Mask request: 0, mask reply: 0, info request: 0, info reply: 0,
  Parameter problem: 0, source quench: 0, timestamp: 0,
  Timestamp response: 0, time exceeded: 0,
  Irdp solicitation: 0, irdp advertisement: 0
Reception:
  Redirect: 2, unreachable: 22048, echo request: 0, echo reply: 0,
```

Review Draft -- Cisco Confidential

```
  Mask request: 0, mask reply: 0, info request: 0, info reply: 0,
  Parameter problem: 0, source quench: 0, timestamp: 0,
  Timestamp response: 0, time exceeded: 0,
  Irdp solicitation: 0, irdp advertisement: 0,
  Format error: 0, checksum error: 0

Statistics last reset: never

switch(config)#
```

Related Commands

Command	Description
show ip process	Displays information about the IP process.

Review Draft -- Cisco Confidential

show running-config ospf

To display the running configuration for Open Shortest Path First version 2 (OSPFv2) for IPv4 networks, use the **show running-config ospf** command.

show running-config ospf

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the running configuration for OSPF:

Need new output

```
switch# show running-config ospf

!Command: show running-config ospf
!Time: Tue Apr 15 09:09:15 2008

version 5.0(3)N1(1)
feature ospf

router ospf 201
  router-id 192.0.2.1
  default-information originate route-map DefaultRouteFilter
  area 0.0.0.10 virtual-link 192.0.2.3
    authentication message-digest
    authentication-key 3 15e76ee89406ccbf
    message-digest-key 21 md5 3 15e76ee89406ccbf
    dead-interval 50
    hello-interval 25
    retransmit-interval 50
    transmit-delay 2
  redistribute bgp 1 route-map FilterExtBGP
  redistribute maximum-prefix 1000 75 warning-only
  area 0.0.0.10 authentication
  area 0.0.0.10 default-cost 25
  area 0.0.0.10 filter-list route-map FilterLSAs in
  log-adjacency-changes
  maximum-paths 3
```

Review Draft -- Cisco Confidential

```
  default-metric 25

interface Ethernet1/5
  ip ospf authentication key-chain Test1
  ip ospf authentication-key 3 15e76ee89406ccbf
  ip ospf message-digest-key 21 md5 3 15e76ee89406ccbf
  ip ospf cost 25
  ip ospf dead-interval 50
  ip ospf hello-interval 25
  ip ospf passive-interface
  ip ospf priority 25
  ip ospf mtu-ignore
  ip router ospf 201 area 0.0.0.15

switch#
```

Related Commands

Command	Description
router ospf	Creates an OSPF instance.

Review Draft -- Cisco Confidential

show vrf

To display the virtual routing and forwarding (VRF) instances, use the **show vrf** command.

show vrf

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the VRF instances configured on the switch:

```
switch# show vrf
VRF-Name                           VRF-ID State   Reason
default                                 1 Up      --
management                              2 Up      --
switch#
```

Related Commands

Command	Description
vrf	Configures a VRF instance.
vrf context	Creates a VRF instance.
vrf member	Adds an interface to a VRF.

Review Draft -- Cisco Confidential

show vrf detail

To display the detailed information of virtual routing and forwarding (VRF) instances, use the **show vrf detail** command.

show vrf detail

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

By default, this command displays the detailed information of the default VRF and management VRF.

This command does not require a license.

Examples

This example shows how to display the detailed information of VRF instances configured on the switch:

```
switch# show vrf detail
VRF-Name: default, VRF-ID: 1, State: Up
    Table-ID: 0x80000001, AF: IPv6, Fwd-ID: 0x80000001, State: Up
    Table-ID: 0x00000001, AF: IPv4, Fwd-ID: 0x00000001, State: Up

VRF-Name: management, VRF-ID: 2, State: Up
    Table-ID: 0x80000002, AF: IPv6, Fwd-ID: 0x80000002, State: Up
    Table-ID: 0x00000002, AF: IPv4, Fwd-ID: 0x00000002, State: Up

switch#
```

Related Commands

Command	Description
vrf	Configures a VRF instance.
vrf context	Creates a VRF instance.
vrf member	Adds an interface to a VRF.

Review Draft -- Cisco Confidential

show vrf interface

To display the virtual routing and forwarding (VRF) information for interfaces, use the **show vrf interface** command.

show vrf interface [**mgmt** *mgmt-number* | **vlan** *vlan-ID*]

Syntax Description

mgmt *mgmt-number*	(Optional) Displays the management interfaces that are added to a VRF. The management interface number is 0.
vlan *vlan-ID*	(Optional) Displays the VLAN interfaces that are added to a VRF. The VLAN interface range is from 1 to 4094.

Command Default

All interfaces

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the VRF information for all configured interfaces:

```
switch# show vrf interface
Interface                  VRF-Name                        VRF-ID
Vlan1                      default                              1
Vlan5                      default                              1
loopback1                  default                              1
mgmt0                      management                           2
switch#
```

This example shows how to display the VRF information for management interfaces:

```
switch# show vrf interface mgmt 0
Interface                  VRF-Name                        VRF-ID
mgmt0                      management                           2
switch#
```

This example shows how to display the VRF information for VLAN interfaces:

```
switch# show vrf interface vlan 1
Interface                  VRF-Name                        VRF-ID
Vlan1                      default                              1
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
vrf member	Adds an interface to a VRF.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

T Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with T.

Review Draft -- Cisco Confidential

timers lsa-arrival (OSPF)

To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the **timers lsa-arrival** command. To return to the default, use the **no** form of this command.

timers lsa-arrival *milliseconds*

no timers lsa-arrival

Syntax Description

milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.

Command Default

1000 milliseconds

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers lsa arrival** command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.

We recommend that you keep the *milliseconds* value of the **timers lsa-arrival** command less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa** command.

This command requires the LAN Base Services license.

Examples

This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:

```
switch(config)# router ospf 1
switch(config-router)# timers lsa-arrival 2000
switch(config-router)#
```

Related Commands

Command	Description
show ip ospf	Displays OSPF information.
timers throttle lsa	Sets rate-limiting values for LSAs being generated.

Review Draft -- Cisco Confidential

timers lsa-group-pacing (OSPF)

To change the interval at which Open Shortest Path First (OSPF) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** command. To return to the default, use the **no** form of this command.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing

Syntax Description

seconds	Time (in seconds) in the interval in which LSAs are grouped and refreshed, checksummed, or aged. The range is from 1 to 1800 seconds. The default value is 240 seconds.

Command Default

The default interval for this command is 240 seconds. OSPF LSA group pacing is enabled by default.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers lsa-group-pacing** command to control the rate at which LSA updates occur and reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPF packet pacing timers are suitable for the majority of OSPF deployments. Do not change the packet pacing timers unless you have tried all other options to meet OSPF packet flooding requirements. You should try summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. There are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis.

Cisco Nexus 6000 groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs that the router is handling. For example, if you have about 10,000 LSAs, you should decrease the pacing interval. If you have a very small database (40 to 100 LSAs), you should increase the pacing interval to 10 to 20 minutes.

This command requires the LAN Base Services license.

Examples

This example shows how to configure OSPF group packet-pacing updates between LSA groups to occur in 60-second intervals for OSPF routing process 1:

```
switch(config)# router ospf 1
```

Review Draft -- Cisco Confidential

```
switch(config-router)# timers lsa-group-pacing 60
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays general information about OSPF routing processes.

Review Draft -- Cisco Confidential

timers throttle lsa (OSPF)

To set rate-limiting values for Open Shortest Path First (OSPF) link-state advertisement (LSA) generation, use the **timers throttle lsa** command. To return to the default values, use the **no** form of this command.

timers throttle lsa *start-time hold-interval max-time*

no timers throttle lsa

Syntax Description

start-time	Start time (in milliseconds) that is used to calculate the subsequent rate limiting times for LSA generation. The range is from 0 to 5000 milliseconds. The default value is 0 milliseconds.
hold-interval	Incremental time (in milliseconds) that is used to calculate the subsequent rate limiting times for LSA generation. The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds.
max-time	Maximum time (in milliseconds) that is used to calculate the subsequent rate limiting times for LSA generation. The range is from 50 to 30,000 milliseconds. The default value is 5000 milliseconds.

Command Default

start-time: 0 milliseconds
hold-interval: 5000 milliseconds
max-time: 5000 milliseconds

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers throttle lsa** command to rate-limit LSA generation.

This command requires the LAN Base Services license.

Examples

This example shows how to customize OSPF LSA throttling:

```
switch(config)# router ospf 1
switch(config-router)# timers throttle lsa 50 5000 6000
switch(config-router)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays information about OSPF routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.

Review Draft -- Cisco Confidential

timers throttle spf (OSPF)

To set the shortest-path first (SPF) best-path schedule initial delay time and the minimum hold between SPF best-path calculation for Open Shortest Path First (OSPF), use the **timers throttle spf** command. To turn off SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	Initial SPF schedule delay in milliseconds. The range is from 1 to 600,000 milliseconds.
spf-hold	Minimum hold time between two consecutive SPF calculations. The range is from 1 to 600,000 milliseconds.
spf-max-wait	Maximum wait time between two consecutive SPF calculations. The range is from 1 to 600,000 milliseconds.

Command Default

SPF throttling is not set.

Command Modes

Router configuration mode

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **timers throttle spf** command to set the SPF timers.

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-maximum* argument. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

Examples

This example shows how to configure a router configured with the start, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1,000, and 90,000 milliseconds:

```
switch(config)# router ospf 1
switch(config-router)# timers throttle spf 5 1000 90000
switch(config-router)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration changes to the startup configuration file.
show ip ospf	Displays information about OSPF routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.
timers throttle lsa	Sets the rate limit for generating LSAs.

Review Draft -- Cisco Confidential

transmit-delay (OSPF virtual link)

To set the estimated time required to end a link-state update packet on the interface, use the **transmit-delay** command. To return to the default, use the **no** form of this command.

transmit-delay *seconds*

no transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Command Default

1 second

Command Modes

Virtual link mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **transmit-delay** command in virtual link configuration to account for the transmission and propagation delays for the virtual link.

This command requires the LAN Base Services license.

Examples

This example sets the retransmit delay value to 3 seconds:

```
switch(config)# router ospf 201
switch(config-router)# area 22 virtual-link 192.0.2.1
switch(config-router-vlink)# transmit-delay 3
```

Related Commands

Command	Description
show ip ospf	Displays general information about Open Shortest Path First (OSPF) routing instances.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

V Commands

This chapter describes the Cisco NX-OS Open Shortest Path First (OSPF) commands that begin with V.

Review Draft -- Cisco Confidential

vrf

To enter a virtual routing and forwarding (VRF) configuration mode and configure submode commands, use the **vrf** command. To remove a VRF instance or disable the VRF configuration mode, use the **no** form of this command.

vrf *name* | **management**

no vrf *name* | **management**

Syntax Description

name	Name of the VRF. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.
management	Specifies the management VRF.

Command Default

None

Command Modes

Address-family configuration mode
Router configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The VRF does not become active until you create an identically named VRF in global configuration mode.

When you enter the VRF configuration mode, the following commands are available:

- **area**—(OSPF) Configures area properties.
- **address-family**—(BGP) Configures an address-family. See the **address-family (BGP)** command for additional information.
- **auto-cost**—(OSPF) Calculates OSPF cost according to bandwidth.
- **cluster-id** {*cluster-id* | *cluster-ip-addr*}—(BGP) Configures the Route Reflector Cluster-ID (router, vrf). Range: 1 to 4294967295. You can enter the cluster identification as a 32-bit quantity or as an IP address. To remove the cluster ID, use the **no** form of this command. Together, a route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.

  The **cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors, which allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.

Review Draft -- Cisco Confidential

Note All route reflectors must maintain stable sessions between all peers in the cluster. If stable sessions cannot be maintained, you should use overlay route reflector clusters instead (route reflectors with different cluster IDs).

- **default-information**—(OSPF) Controls the distribution of the default route. See the **default-information originate (OSPF)** command for additional information.
- **default-metric**—(OSPF) Specifies the default metric for redistributed routes. See the **default-metric (OSPF)** command for additional information.
- **distance**—(OSPF) Defines the OSPF administrative distance. See the **distance (OSPF)** command for additional information.
- **exit**—(BGP) Exits from the current command mode.
- **log-adjacency-changes**—(OSPF) Logs changes in adjacency state.
- **log-neighbor-changes**—Enables logging of the BGP neighbor resets. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command. The **log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

  Using the **log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the internal buffer of the router, and are not stored to the disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

  The neighbor status change messages are not tracked if the bgp **log-neighbor-changes** command is disabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** command.

  The **eigrp log-neighbor-changes** command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the bgp **log-neighbor-changes** command.

  Use the **show logging command** to display the log for the BGP neighbor changes.
- **max-metric**—(OSPF) Maximizes the cost metric. See the **max-metric (OSPF)** command for additional information.
- **maximum-paths**—(OSPF) Sets the maximum number of parallel routes that OSPF can support. See the **maximum-paths (OSPF)** command for additional information.
- **neighbor**—Configures a BGP neighbor. See the **neighbor** command for additional information.
- **no**—Negates a command or set its defaults.
- **redistribute**—(OSPF) Redistributes information from another routing protocol. See the **redistribute (OSPF)** command for additional information.
- **rfc1583compatibility**—(OSPF) Configures RFSC 1583 compatibility for external path preferences. See the **rfc1583compatibility** command for additional information.
- **router-id** *ip-addr*—Specifies the IP address to use as the router-id.

Review Draft -- Cisco Confidential

- **shutdown**—(OSPF) Shuts down the OSPF protocol instance. See the **shutdown (OSPF)** command for additional information.
- **summary-address**—(OSPF) Configures route summarization for redistribution. See the **summary-address (OSPF)** command for additional information.
- **timers** *bestpath-timeout*—Configures the best-path timeout in seconds. Range: 1 to 3600. Default: 300.

Examples

This example shows how to enter VRF configuration mode in a BGP environment:

```
switch(config)# router bgp 100
switch(config-router)# vrf management
switch(config-router-vrf)#
```

This example shows how to enter VRF configuration mode in an OSPF environment:

```
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)# router ospf 201
switch(config-router)# vrf RemoteOfficeVRF
switch(config-router-vrf)#
```

Related Commands

Command	Description
vrf context	Creates a VRF.
show vrf	Displays the VRF configuration information.

Review Draft -- Cisco Confidential

vrf context

To create a virtual routing and forwarding instance (VRF) and enter VRF configuration mode, use the **vrf context** command. To remove a VRF entry, use the **no** form of this command.

vrf context {*name* | **management**}

no vrf context {*name* | **management**}

Syntax Description

name	Name of the VRF. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.
management	Specifies the management VRF.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to create a VRF context:

```
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)#
```

Related Commands

Command	Description
vrf	Creates or configures a VRF instance.
show vrf	Displays the VRF configuration information.

Review Draft -- Cisco Confidential

vrf member

To add an interface to a virtual routing and forwarding (VRF) instance or to configure object tracking on a VRF instance, use the **vrf member** command. To remove the object tracking for this route, use the **no** form of this command.

vrf member *vrf-name*

no vrf member *vrf-name*

Syntax Description

vrf-name	VRF name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Interface configuration mode
Object tracking confiuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **vrf member** command in object tracking configuration mode to track objects in a nondefault VRF.

Examples

This example shows how to track an IP route in VRF Red:

```
switch(config)# track 1 ip route 10.10.10.0/8 reachability
switch(config-track)# vrf member Red
switch(config-track)#
```

This example shows how to add the Ethernet interface 1/5 to VRF RemoteOfficeVRF:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)#
```

Related Commands

Command	Description
show vrf	Displays the VRF configuration information.

<I_Italic>Review Draft -- Cisco Confidential

PART 7

RIP Commands

Review Draft -- Cisco Confidential

A Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with A.

Review Draft -- Cisco Confidential

address-family (RIP)

To configure an address family for the Routing Information Protocol (RIP), use the **address-family** command in router configuration mode.

address-family ipv4 unicast

Syntax Description

ipv4	Specifies the IPv4 address family.
unicast	Specifies unicast address support.

Command Default

This command has no default settings.

Command Modes

Router configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to set the IPv4 unicast address family for a RIP instance:

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
```

Related Commands

Command	Description
default-information	Controls the distribution of a default route.
default-metric	Configures the default metric for routes redistributed into RIP.
distance	Configures the administrative distance.
maximum-paths	Configures the maximum number of equal-cost paths.
redistribute	Configures route redistribution for RIP.
show ip rip	Displays a summary of RIP information for all RIP instances.
timers	Configures the RIP timers.

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with C.

Review Draft -- Cisco Confidential

clear ip rip policy statistics redistribute

To clear policy statistics for routes redistributed into the Routing Information Protocol (RIP) topology table, use the **clear ip rip policy statistics redistribute** command in any mode.

clear ip rip policy statistics redistribute {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **static**} [**vrf** *vrf-name*]

Syntax Description

bgp	Clears policy statistics for the Border Gateway Protocol (BGP).
direct	Clears policy statistics for directly connected routes only.
eigrp	Clears policy statistics for the Enhanced Interior Gateway Routing Protocol (EIGRP).
ospf	Clears policy statistics for the Open Shortest Path First (OSPF) protocol.
static	Clears policy statistics for IP static routes.
id	For the **bgp** keyword, an autonomous system number. The range for 2-byte numbers is from 1 to 65535. The range for 4-byte numbers is from 1.0 to 65535.65535. For the **eigrp** keyword, an EIGRP instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string. For the **ospf** keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name can be a maximum of 32 alphanumeric characters and is case-sensitive.

Command Default

This command has no default settings.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear policy statistics for EIGRP:

```
switch# clear ip rip policy statistics redistribute eigrp 201
```

Related Commands

Command	Description
show ip rip policy statistics	Displays policy statistics for RIP.

Review Draft -- Cisco Confidential

clear ip rip statistics

To clear the Routing Information Protocol (RIP) statistics, use the **clear ip rip statistics** command in any mode.

clear ip rip statistics [**interface** *type instance*] [**vrf** *vrf-name*]

Syntax Description

interface *type instance*	(Optional) Specifies the interface to clear topology entries.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name can be up to 32 alphanumeric characters.

Command Default

This command has no default settings.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear all RIP statistics:

```
switch# clear ip rip statistics
```

Related Commands

Command	Description
show rip statistics	Displays database and interface entry information for the RIP process.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

D Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with D.

Review Draft -- Cisco Confidential

default-information originate (RIP)

To generate a default route into the Routing Information Protocol (RIP), use the **default-information originate** command. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**route-map** *map-name*]

no default-information originate

Syntax Description

always	(Optional) Generates the default route if the route is not in the RIP routing information base.
route-map *map-name*	(Optional) Generates the default route only if the route is permitted by the route map. The map name is any alphanumerical string up to 63 characters.

Command Default

Disabled

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to originate a default route (0.0.0.0/0) to all routes that pass the Condition route map:

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# default-information originate route-map Condition
switch(config-router-af)#
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
default-metric	Sets the metric for routes redistributed into RIP.
redistribute	Redistributes routes from other routing protocols into RIP.
show ip rip route	Displays the routes in RIP table.

Review Draft -- Cisco Confidential

default-metric (RIP)

To set default metric values for the Routing Information Protocol (RIP), use the **default-metric** command in router address-family configuration mode. To return to the default state, use the **no** form of this command.

default-metric *value*

no default-metric [*value*]

Syntax Description

value	Default metric value. The range is from 1 to 15.

Command Default

value: 1

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **default-metric** command with the **redistribute** command to use the same metric value for all redistributed routes. A default metric helps to solve the problem of redistributing routes with incompatible metrics. Whenever external metrics do not convert to RIP metrics, you can use a default metric to provide a reasonable substitute to the external metric and enable the redistribution to proceed.

Examples

This example shows how to advertise Open Shortest Path First (OSPF) routes using RIP and assign the OSPF-derived routes with a RIP metric of 10:

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# default-metric 10
switch(config-router-af)# redistribute ospf 109 route-map FilterOSPF
switch(config-router-af)#
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
copy running-config startup-config	Saves the configuration to the startup configuration file.
default-information originate	Generates a default route for routes redistributed into RIP.
redistribute	Redistributes routes from one routing domain into another routing domain.
show ip rip route	Displays the routes in RIP table.

Review Draft -- Cisco Confidential

distance (RIP)

To define the administrative distance assigned to routes discovered by the Routing Information Protocol (RIP), use the **distance** command. To remove the distance and restore the system to its default condition, use the **no** form of this command.

distance *admin-distance*

no distance *admin-distance*

Syntax Description

admin-distance	Administrative distance to be assigned to RIP routes. The range is from 1 to 255.

Command Default

admin-distance: 120

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **distance** command to change the preference of RIP routes over other protocol routes. Numerically, an administrative distance is an integer from 1 to 255. In general, a higher value indicates a lower trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored.

Examples

This example shows how to set the administrative distance for RIP:

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# distance 85
switch(config-router-af)#
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
redistribute	Redistributes routes from one routing domain into RIP.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with F.

Review Draft -- Cisco Confidential

feature rip

To enable the Routing Information Protocol (RIP), use the **feature rip** command. To disable RIP, use the **no** form of this command.

feature rip

no feature rip

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the RIP feature before you can configure RIP.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to enable the RIP feature:

```
switch# configure terminal
switch(config)# feature rip
switch(config)#
```

This example shows how to disable the RIP feature:

```
switch# configure terminal
switch(config)# no feature rip
switch(config)#
```

Related Commands

Command	Description
router rip	Creates a RIP instance.
show feature	Displays the status of features on a switch.
show rip	Displays RIP configuration information.

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with I.

Review Draft -- Cisco Confidential

ip rip authentication key-chain

To enable authentication for the Routing Information Protocol (RIP) Version 2 packets and to specify the set of keys that can be used on an interface, use the **ip rip authentication key-chain** command. To prevent authentication, use the **no** form of this command.

ip rip authentication key-chain *name-of-chain*

no ip rip authentication key-chain [*name-of-chain*]

Syntax Description

name-of-chain	Group of valid keys.

Command Default

No authentication is provided for RIP packets.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to configure the interface to accept and send any key that belongs to the key-chain trees:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip rip authentication key-chain trees
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
key-chain	Creates a set of keys that can be used by an authentication method.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

ip rip authentication mode

To specify the type of authentication used in the Routing Information Protocol (RIP) Version 2 packets, use the **ip rip authentication mode** command. To restore clear text authentication, use the **no** form of this command.

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

Syntax Description

text	Specifies the clear text authentication.
md5	Specifies the message Digest 5 (MD5) authentication.

Command Default

Clear text authentication is provided for RIP packets if you configured a key chain.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to configure the interface to use MD5 authentication:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip rip authentication mode md5
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
key chain	Enables authentication for routing protocols.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

ip rip metric-offset

To add an additional value to the incoming IP Routing Information Protocol (RIP) route metric for an interface, use the **ip rip metric-offset** command. To return the metric to its default value, use the **no** form of this command.

ip rip metric-offset *value*

no ip rip metric-offset

Syntax Description

value	Value to add to the incoming route metric for an interface. The range is from 1 to 15. The default is 1.

Command Default

value: 1

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip route metric-offset** command to influence which routes are used by Cisco Nexus 6000. This command allows you to add a fixed offset to the route metric of all incoming routes on an interface. For example, if you set the metric-offset to 5 on an interface and the incoming route metric is 5, then Cisco Nexus 6000 adds the route to the route table with a metric of 10.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to configure a metric offset of 10 for all incoming RIP routes on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip rip metric-offset 10
switch(config-if)#
```

Related Commands

Command	Description
ip rip offset-list	Adds an offset value to incoming RIP route metrics.

Review Draft -- Cisco Confidential

ip rip offset-list

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the **ip rip offset-list** command. To remove an offset list, use the **no** form of this command.

ip rip offset-list *value*

no ip rip offset-list

Syntax Description

value	Value to add to the incoming route metric for an interface. The range is from 1 to 15. The default is 1.

Command Default

value: 1

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to configure an offset of 10 for all incoming RIP routes on Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip rip offset-list 10
switch(config-if)#
```

Related Commands

Command	Description
ip rip metric-offset	Adds an offset value to incoming RIP route metrics.

Review Draft -- Cisco Confidential

ip rip passive-interface

To suppress the sending of the Routing Information Protocol (RIP) updates on an interface, use the **ip rip passive-interface** command. To unsuppress updates, use the **no** form of this command.

ip rip passive-interface

no ip rip passive-interface

Syntax Description

This command has no arguments or keywords.

Command Default

RIP updates are sent on the interface.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

While RIP stops sending routing updates to the multicast (or broadcast) address on a passive interface, RIP continues to receive and process routing updates from its neighbors on that interface.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to configure Ethernet 1/2 as a passive interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip rip passive-interface
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

ip rip poison-reverse

To enable poison-reverse processing of the Routing Information Protocol (RIP) router updates, use the **ip rip poison-reverse** command. To disable poison-reverse processing of RIP updates, use the **no** form of this command.

ip rip poison-reverse

no ip rip poison-reverse

Syntax Description

This command has no arguments or keywords.

Command Default

Split horizon is always enabled. Poison-reverse processing is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip rip poison-reverse** command to enable poison-reverse processing of RIP router updates. By default, Cisco Nexus 6000 does not advertise RIP routes out the interface over which they were learned (split horizon). If you configure both poison reverse and split horizon, then Cisco Nexus 6000 advertises the learned routes as unreachable over the interface on which the route was learned.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to enable poison-reverse processing for an interface running RIP:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip rip poison-reverse
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

ip rip route-filter

To filter the Routing Information Protocol (RIP) routes coming in or out of an interface, use the **route-filter** command. To remove filtering from an interface, use the **no** form of this command.

ip rip route filter {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

no ip rip route filter {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

Syntax Description

prefix-list *list-name*	Associates a prefix list to filter RIP packets.
route-map *map-name*	Associates a route map to set the redistribution policy for RIP.
in	Filters incoming routes.
out	Filters outgoing routes.

Command Default

Route filtering is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip rip route-filter** command to filter incoming or outgoing routes on an interface.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to use a route map to filter routes for a RIP interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip rip route-filter route-map InRipFilter in
switch(config-if)#
```

Related Commands

Command	Description
prefix-list	Creates a prefix list.
route-map	Creates a route map.

Review Draft -- Cisco Confidential

ip rip summary-address

To configure a summary aggregate address under an interface for the Routing Information Protocol (RIP), use the **ip rip summary-address** command. To disable summarization of the specified address or subnet, use the **no** form of this command.

ip rip summary-address *ip-prefix/mask*

no ip rip summary-address *ip-prefix/mask*

Syntax Description

ip-prefix/length	IP prefix and prefix length to be summarized.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip rip summary-address** command summarizes an address or subnet under a specific interface.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to configure the summary address 192.0.2.0 that is advertised out Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip summary-address rip 192.0.2.0/24
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

ip router rip

To specify the Routing Information Protocol (RIP) instance for an interface, use the **ip router rip** command. To return to the default, use the **no** form of this command.

ip router rip *instance-tag*

no ip router rip *instance-tag*

Syntax Description

instance-tag	Name of the RIP instance. The *instance-tag* can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, make sure that you enable RIP on the switch.

This command requires the LAN Base Services license.

Examples

This example shows how to set the RIP instance for an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router rip Enterprise
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration to the startup configuration file.
feature rip	Enables RIP on the switch.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

M Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with M.

Review Draft -- Cisco Confidential

maximum-paths (RIP)

To configure the maximum number of equal cost parallel routes that the Routing Information Protocol (RIP) can install into the routing table, use the **maximum-paths** command. To remove the **maximum-paths** command and restore the system to its default condition, use the **no** form of this command.

maximum-paths *maximum*

no maximum-paths

Syntax Description

maximum	Maximum number of parallel routes that RIP can install in a routing table. The range is from 1 to 16.

Command Default

8 paths

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to allow a maximum of 16 equal cost paths to a destination:

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# maximum-paths 16
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
copy running-config startup-config	Saves the configuration to the startup configuration file.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

R Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with R.

Review Draft -- Cisco Confidential

redistribute (RIP)

To redistribute routes from another routing domain into the Routing Information Protocol (RIP), use the **redistribute** command. To restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

redistribute {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **static**} **route-map** *map-name*

Syntax Description

bgp *id*	Redistributes routes from the Border Gateway Protocol (BGP). The ID is an autonomous system number. The range for 2-byte numbers is from 1 to 65535. The range for 4-byte numbers is from 1.0 to 65535.65535.
direct	Redistributes routes from directly connected routes only.
eigrp *id*	Redistributes routes from the Enhanced Interior Gateway Routing Protocol (EIGRP). The ID is an EIGRP instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string.
ospf *id*	Redistributes routes from the Open Shortest Path First (OSPF) protocol. The ID is an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
static	Redistributes routes from IP static routes.
route-map *map-name*	Associates a route map to set the redistribution policy for RIP.

Command Default

Route redistribution is disabled.

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Cisco Nexus 6000 filters redistributed routing information using a route map. You can configure the route map to set the RIP metric used for redistributed routes. If you do not set the RIP metric with a route map, Cisco Nexus 6000 determines the metric based on the redistributed protocol or by the **default-metric** command. If Cisco Nexus 6000 cannot determine a valid metric, then it does not redistribute the routes.

Examples

This example shows how to redistribute BGP routes into a RIP process:

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute bgp 64496
switch(config-router-af)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
default-information originate	Generates a default route for routes redistributed into RIP.
default-metric	Sets default metric values for routes redistributed from other protocols into RIP.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

restart (RIP)

To restart a Routing Information Protocol (RIP) instance and remove all associated neighbors, use the **restart** command.

restart eigrp *instance-tag*

Syntax Description

instance-tag	Name for an RIP routing instance. The name can be a maximum of 20 alphanumeric characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to restart the RIP instance and remove all neighbors:

```
switch(config)# restart rip Enterprise
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the configuration in the startup configuration file.
show ip eigrp interfaces	Displays information about EIGRP interfaces.

Review Draft -- Cisco Confidential

router rip

To configure the Routing Information Protocol (RIP) routing process, use the **router rip** command. To turn off the RIP routing process, use the **no** form of this command.

router rip *instance-tag*

no router rip

Syntax Description

instance-tag	Name for this RIP instance.

Command Default

No RIP routing process is defined.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to begin the RIP routing process:

```
switch(config)# router rip Enterprise
```

Related Commands

Command	Description
ip router rip	Specifies a RIP instance for an interface.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) **show** commands.

Review Draft -- Cisco Confidential

show ip rip

To display the configuration and status of the Routing Information Protocol (RIP), use the **show ip rip** command in any mode.

show ip rip [*instance-tag*] [**vrf** *vrf-name*]

Syntax Description

instance-tag	(Optional) RIP instance. The instance tag can be a maximum of 20 alphanumeric characters.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

No default behavior or values

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the RIP configuration information:

```
switch(config-if)# show ip rip
```

Related Commands

Command	Description
show ip rip interface	Displays RIP information for an interface.
show ip rip neighbor	Displays RIP neighbor information.
show ip rip policy statistics	Displays RIP policy statistics.
show ip rip route	Displays RIP route information.
show ip rip statistics	Displays RIP statistics.

Review Draft -- Cisco Confidential

show ip rip interface

To display interface entry information from the Routing Information Protocol (RIP) topology table, use the **show ip rip interface** command in any mode.

show ip rip interface [*type slot/port*] [**vrf** *vrf-name*]

Syntax Description

interface *type slot/port*	(Optional) Specifies the interface.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

This command has no default settings.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the neighbor information for a specified interface from the RIP topology table:

```
switch(config-if)# show ip rip interface ethernet 1/2
```

Related Commands

Command	Description
show ip rip	Displays RIP information.
show ip rip neighbor	Displays RIP neighbor information.
show ip rip policy statistics	Displays RIP policy statistics.
show ip rip route	Displays RIP route information.
show ip rip statistics	Displays RIP statistics.

Review Draft -- Cisco Confidential

show ip rip neighbor

To display the neighbor information from the Routing Information Protocol (RIP) topology table, use the **show ip rip neighbor** command in any mode.

show ip rip neighbor [*interface-type instance*] [**vrf** *vrf-name*]

Syntax Description

interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
instance	(Optional) Either a physical interface instance or a virtual interface instance.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

No default behavior or values

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

The following is sample output from the **show rip neighbor** command:

```
switch(config-if)# show ip rip neighbor
```

Related Commands

Command	Description
show ip rip	Displays RIP information.
show ip rip interface	Displays RIP information for an interface.
show ip rip policy statistics	Displays RIP policy statistics.
show ip rip route	Displays RIP route information.
show ip rip statistics	Displays RIP statistics.

Review Draft -- Cisco Confidential

show ip rip policy statistics

To display the policy statistics for the Routing Information Protocol (RIP), use the **show ip rip policy statistics** command in any mode.

show ip rip policy statistics redistribute {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **static**} [**vrf** *vrf-name*]

Syntax Description

bgp	Displays policy statistics for the Border Gateway Protocol (BGP).
direct	Displays policy statistics for directly connected routes only.
eigrp	Displays policy statistics for Enhanced Interior Gateway Routing Protocol (EIGRP).
ospf	Displays policy statistics for Open Shortest Path First (OSPF) protocol.
static	Displays policy statistics for IP static routes.
id	For the **bgp** keyword, an autonomous system number. The range for 2-byte numbers is from 1 to 65535. The range for 4-byte numbers is from 1.0 to 65535.65535. For the **eigrp** keyword, an EIGRP instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string. For the **ospf** keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. You can enter a decimal number, but Cisco Nexus 6000 stores it internally as a string.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

No default behavior or values.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to show policy statistics for EIGRP:

```
switch# show ip rip policy statistics redistribute eigrp 201
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear ip rip policy statistics	Clears policy statistics for RIP.
show ip rip	Displays RIP information.
show ip rip interface	Displays RIP information for an interface.
show ip rip neighbor	Displays RIP information for a neighbor.
show ip rip route	Displays RIP route information.
show ip rip statistics	Displays RIP statistics.

Review Draft -- Cisco Confidential

show ip rip route

To display route information from the Routing Information Protocol (RIP) topology table, use the **show ip rip route** command in any mode.

show ip rip route [*prefix/length*] [**summary**] [**vrf** *vrf-name*]

Syntax Description

prefix/length	(Optional) IP prefix about which routing information should be displayed.
summary	(Optional) Displays information about summary routes.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

No default behavior or values

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display route information from the RIP topology table:

```
switch# show ip rip route
```

Related Commands

Command	Description
show ip rip	Displays RIP information.
show ip rip interface	Displays RIP information for an interface.
show ip rip neighbor	Displays RIP information for a neighbor.
show ip rip policy statistics	Displays policy statistics for RIP.
show ip rip statistics	Displays RIP statistics.

Review Draft -- Cisco Confidential

show ip rip statistics

To display statistical entry information from the Routing Information Protocol (RIP) topology table, use the **show ip rip statistics** command in any mode.

show ip rip statistics [*interface-type instance*] [**vrf** *vrf-name*]

Syntax Description

interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
instance	(Optional) Either a physical interface instance or a virtual interface instance.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

No default behavior or values.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the RIP statistics:

```
switch# show ip rip statistics
```

Related Commands

Command	Description
show ip rip	Displays RIP information.
show ip rip interface	Displays RIP information for an interface.
show ip rip neighbor	Displays RIP information for a neighbor.
show ip rip policy statistics	Displays policy statistics for RIP.
show ip rip route	Displays RIP route information.

Review Draft -- Cisco Confidential

T Commands

This chapter describes the Cisco NX-OS Routing Information Protocol (RIP) commands that begin with T.

Review Draft -- Cisco Confidential

timers basic

To adjust the Routing Information Protocol (RIP) network timers, use the **timers basic** command. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush*

no timers basic

Syntax Description

update	Rate (in seconds) at which updates are sent. The range is from 5 to 4,294,967,295. The default is 30 seconds.
invalid	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when no updates refresh the route. The route then enters into a *holddown* state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. The range is from 1 to 4,294,967,295. The default is 180 seconds.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed; it should be at least three times the value of the *update* argument. A route enters into a *holddown* state when an update packet is received that indicates that the route is unreachable. The route is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The range is from 0 to 4,294,967,295. The default is 180 seconds.
flush	Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the sum of the *invalid* argument plus the *holddown* argument. If it is less than this sum, the proper *holddown* interval cannot elapse, which results in a new route being accepted before the *holddown* interval expires. The range is from 1 to 4,294,967,295. The default is 240 seconds.

Command Default

update: 30 seconds
invalid: 180 seconds
holddown: 180 seconds
flush: 240 seconds

Command Modes

Router address-family configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can modify the basic timing parameters for RIP. These timers must be the same for all routers and servers in the network.

Review Draft -- Cisco Confidential

Note You can view the current and default timer values by using the **show ip protocols** command.

Examples

This example shows how to set updates to broadcast every 5 seconds. If Cisco Nexus 6000 does not hear from a router in 15 seconds (the invalid time), it declares the route as unusable. Cisco Nexus 6000 suppresses further information for an additional 15 seconds (the holddown time). At the end of the suppression period, Cisco Nexus 6000 flushes the route from the routing table.

```
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# timers basic 5  15  15  30
switch(config-router-af)#
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
copy running-config startup-config	Saves the configuration to the startup configuration file.
show ip rip	Displays a summary of RIP information for all RIP instances.

Review Draft -- Cisco Confidential

<I_Italic>Review Draft -- Cisco Confidential

PART 8

Unicast RIB and FIB Commands

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS unicast Routing Information Base (RIB) and the Forwarding Information Base (FIB) commands that begin with C.

Review Draft -- Cisco Confidential

clear forwarding route

To clear forwarding information, use the **clear forwarding route** command.

clear forwarding {**ip** | **ipv4**} **route** [* | *prefix*] [**vrf** *vrf-name*]

Syntax Description

ip	Clears an IPv4 route.
ipv4	Clears an IPv4 route.
*	(Optional) Clears all routes.
prefix	(Optional) IPv4 prefix. The IPv4 format is x.x.x.x/length.
vrf *vrf-name*	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clears a route from the FIB:

```
switch# clear forwarding ip 10.0.0.1/8
```

Review Draft -- Cisco Confidential

clear forwarding inconsistency

To clear the Layer 3 inconsistency checker for the Forwarding Information Base (FIB), use the **clear forwarding inconsistency** command.

clear forwarding inconsistency

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear the Layer 3 inconsistency checker for all modules:

```
switch# clear forwarding inconsistency module all
```

Related Commands

Command	Description
show forwarding inconsistency	Displays information about the FIB inconsistencies.
test forwarding inconsistency	Triggers the forwarding inconsistency checker.

Review Draft -- Cisco Confidential

clear ip adjacency statistics

To clear adjacency statistics, use the **clear ip adjacency statistics** command.

clear ip adjacency statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear the adjacency statistics:

```
switch# clear ip adjacency statistics
```

Related Commands

Command	Description
show ip adjacency	Displays adjacency information.

Review Draft -- Cisco Confidential

clear ip route

To clear individual routes from the unicast Routing Information Base (RIB), use the **clear ip route** command.

clear ip route [* | *addr* | *prefix*]] [**vrf** *vrf-name*]

Syntax Description

*	(Optional) Clears all routes.
addr	(Optional) Clears this route. The format is x.x.x.x.
prefix	(Optional) Clears this prefix. The format is x.x.x.x/length.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) context name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **clear ip route** command to clear individual routes from the route table.

Caution The * keyword is severely disruptive to routing.

Examples

This example shows how to clear the individual route:

```
switch(config)# clear ip route 192.0.2.1
```

Related Commands

Command	Description
show ip route	Displays entries in the route table.

Review Draft -- Cisco Confidential

clear sockets statistics

To clear the socket statistics, use the **clear sockets statistics** command.

clear sockets statistics [**all** | **raw** | **tcp** | **udp**]

Syntax Description

all	(Optional) Clears all the socket statistics.
raw	(Optional) Clears the socket statistic for the raw IPv4 protocols.
tcp	(Optional) Clears the socket statistic for the TCP IPv4 protocols.
udp	(Optional) Clears the socket statistic for the UDP IPv4 protocols.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear the TCP socket statistics:

```
switch# clear sockets statistics tcp
```

Related Commands

Command	Description
show sockets client	Displays information about the socket client information.
show sockets connection	Displays information about the socket connection.
show sockets statistics	Displays information about the socket statistics.

Review Draft -- Cisco Confidential

H Commands

This chapter describes the Cisco NX-OS unicast Routing Information Base (RIB) and the Forwarding Information Base (FIB) commands that begin with H.

Review Draft -- Cisco Confidential

hardware profile ucast6 max-limit

To set the maximum number of unicast IPv6 entry limit for the host table, use the **hardware profile ucast6 max-limit** command.

hardware profile ucast6 max-limit *max-limit*

Syntax Description

max-limit	Maximum limit for the unicast IPv6 entries. The range is from 0 to 8000.

Defaults

4000

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **hardware profile ucast6 max-limit** command to limit the maximum number of host entries in the host table.

After setting the limit for multicast and IPv6 in the host table, the remaining number of entries are allocated for IPv4 host entries.

Note A limit set by using the **hardware profile multicast max-limit** command overrides the limit set by using the **hardware profile ucast6 max-limit** command.

This example shows how to set the maximum number of unicast IPv6 entry limit in the host table:

```
switch# configure terminal
switch(config)# hardware profile ucast6 max-limit 2500
Warning!!: The host (v4 & v6) unicast route limits have been changed.
switch(config)#
```

Related Commands

Command	Description
hardware profile multicast max-limit	Sets the maximum number of entries in the multicast routing table.
show hardware profile status	Displays information about the multicast and unicast routing table limits.

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS unicast Routing Information Base (RIB) and the Forwarding Information Base (FIB) commands that begin with I.

Review Draft -- Cisco Confidential

ip load-sharing address

To configure the load-sharing algorithm used by the unicast Forwarding Information Base (FIB), use the **ip load-sharing address** command. To restore the default, use the **no** form of this command.

ip load-sharing address {**destination port destination** | **source-destination** [**port source-destination**]} [**universal-id** *seed*]

no ip load-sharing address {**destination port destination** | **source-destination** [**port source-destination**]} [**universal-id** *seed*]

Syntax Description

destination port destination	Sets the load-sharing algorithm based on the destination address and port.
source-destination	Sets the load-sharing algorithm based on the source and destination address.
port source-destination	(Optional) Sets the load-sharing algorithm based on the source and destination address and port address.
universal-id *seed*	(Optional) Sets the random seed for the load sharing hash algorithm. The range is from 1 to 4294967295.

Command Default

Destination address and port address

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip load-sharing address** command to set the load-sharing algorithm that the unicast FIB uses to select a path from the equal-cost paths in the Routing Information Base (RIB).

Examples

This example shows how to set the load-sharing algorithm to use the source and destination address:

```
switch(config)# ip load-sharing address source-destination
```

Related Commands

Command	Description
show ip load-sharing	Displays the load-sharing algorithm.
show routing hash	Displays the path the RIB and FIB select for a source/destination pair.

Review Draft -- Cisco Confidential

ip route

To configure a static route, use the **ip route** command. To remove the static route, use the **no** form of this command.

ip route *ip-prefix/mask* {[*interface*] *next-hop*} [*preference*] [**tag** *id*]

no ip route *ip-prefix/mask* {[*interface*] *next-hop*} [*preference*] [**tag** *id*]

Syntax Description

ip-prefix/mask	IP prefix and prefix mask. The format is x.x.x.x/length. The length is 1 to 32.
interface	(Optional) Interface on which all packets are sent to reach this route. Use **?** to display a list of supported interfaces.
next-hop	IP address of the next hop that can be used to reach that network. You can specify an IP address and an interface type and interface number. The format is x.x.x.x/length. The length is 1 to 32.
preference	(Optional) Route preference that is used as the administrative distance to this route. The range is from 1 to 255. The default is 1.
tag *id*	(Optional) Assigns a route tag that can be used to match against in a route map. The range is from 0 to 4294967295. The default is 0.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Static routes have a default administrative distance of 1. If you want a dynamic routing protocol to take precidence over a static route, you must configure the static route preference argument to be greater than the administrative distance of the dynamic routing protocol. For example, routes derived with the Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, you should specify an administrative distance greater than 100.

Examples

This example shows how to create a static route for destinations with the IP address prefix 192.168.1.1/32, reachable through the next-hop address 10.0.0.2:

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2
```

This example shows how to assign a tag to the previous example so that you can configure a route map that can match on this static route:

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2 tag 5
```

Review Draft -- Cisco Confidential

This example shows how to choose a preference of 110. In this case, packets for prefix 10.0.0.0 are routed to a router at 172.31.3.4 if dynamic route information with an administrative distance less than 110 is not available.

```
switch# configure terminal
switch(config)# ip route 10.0.0.0/8 172.31.3.4 110
switch(config)#
```

Related Commands

Command	Description
match tag	Matches the tag value associated with a route.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS unicast Routing Information Base (RIB) and the Forwarding Information Base (FIB) **show** commands.

Review Draft -- Cisco Confidential

show forwarding

To display forwarding information, use the **show forwarding** command.

show forwarding [**ip** | **ipv4**] {**adjacency** | **interfaces** | **route** | **trace** [**clear**] | **table** *id* | **pss** | **route**} [**ethernet** | **port-channel** | **vlan** *slot*] [**vrf** *vrf-name*]

Syntax Description

ip	(Optional) Displays the IPv4 forwarding information.
ipv4	(Optional) Displays the IPv4 forwarding information.
adjacency	Displays the adjacency information.
interfaces	Displays the forwarding information for interfaces on a module.
route	Displays the forwarding information for routes on a module.
trace	Displays the forwarding trace buffer on a module.
clear	(Optional) Clears the forwarding trace buffer on a module.
table *id*	Displays the forwarding information for a route table. The *id* range is from 0 to 2147483647.
pss	Displays route information from persistent storage.
route	Displays route information from the IP routing table.
ethernet *slot*	(Optional) Displays information for the ethernet. The slot range depends on the hardware platform.
port-channel *slot*	(Optional) Displays information for the port-channel. The slot range depends on the hardware platform.
vlan	(Optional) Displays information for the vlan. The slot range depends on the hardware platform.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show forwarding** command on the supervisor to view forwarding information on a module. Optionally, you can use the **attach module** command to attach to a module and use the **show forwarding** command on the module.

Review Draft -- Cisco Confidential

Examples

This example shows how to display forwarding information for module 2:

```
switch# show forwarding route ethernet 2
```

Related Commands

Command	Description
show ip fib	Displays information about the FIB.

Review Draft -- Cisco Confidential

show forwarding distribution

To display forwarding distribution information, use the **show forwarding distribution** command.

show forwarding distribution [**clients** | **fib-state**]

Syntax Description

clients	(Optional) Displays the forwarding distribution information for unicast clients.
fib-state	(Optional) Displays the forwarding distribution state for unicast Forwarding Information Base (FIB).

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the forwarding information for unicast clients:

```
switch# show forwarding distribution clients
```

Related Commands

Command	Description
show ip fib distribution	Displays distribution information about the FIB.

Review Draft -- Cisco Confidential

show forwarding distribution multicast

To display information about multicast Forwarding Information Base (FIB) distribution messages, use the **show forwarding distribution multicast** command.

show forwarding distribution multicast [**messages**]

Syntax Description

messages	(Optional) Displays message information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about multicast distribution messages:

```
switch(config)# show forwarding distribution multicast
Number of Multicast FIB Processes Active: 1
Slot     FIB State
   1        ACTIVE
switch#
```

Review Draft -- Cisco Confidential

show forwarding distribution multicast client

To display information about the multicast Forwarding Information Base (FIB) distribution client, use the **show forwarding distribution multicast client** command.

show forwarding distribution multicast client

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the multicast FIB distribution client:

```
switch# show forwarding distribution multicast client
Client-name  Client-id  Shared Memory Name
mrib         1          mrib-mfdm
switch#
```

Review Draft -- Cisco Confidential

show forwarding distribution multicast outgoing-interface-list

To display information about the multicast Forwarding Information Base (FIB) outgoing interface (OIF) list, use the **show forwarding distribution multicast outgoing-interface-list** command.

show forwarding distribution multicast outgoing-interface-list {**L2** | **L3**} [*index*]

Syntax Description

L2	Specifies the Layer 2 OIF list.
L3	Specifies the Layer 3 OIF list.
index	(Optional) OIF list index.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the multicast OIF list for Layer 3:

```
switch# show forwarding distribution multicast outgoing-interface-list L3
```

Review Draft -- Cisco Confidential

show forwarding distribution multicast route

To display information about the multicast Forwarding Information Base (FIB) distribution routes, use the **show forwarding distribution multicast route** command.

show forwarding distribution [**ip** | **ipv4**] **multicast route** [**table** *id* | **vrf** *vrf_name*] [[**group** {*group-addr* [*mask*] | *group-prefix*}] [**source** {*source-addr* [*source-mask*] | *source-prefix*}] | **summary**]

Syntax Description

ip	(Optional) Specifies IPV4 information.
ipv4	(Optional) Specifies IPV4 information.
table *id*	(Optional) Specifies the multicast routing table ID. The range is from 0 to 2147483647.
vrf *vrf_name*	(Optional) Specifies a virtual routing and forwarding (VRF) name. The name can be a maximum of 32 alphanumeric characters.
group	(Optional) Specifies an IPv4 multicast group.
group-addr	IPv4 multicast group address.
mask	(Optional) Mask for the group address.
group-prefix	(Optional) IPv4 multicast group prefix.
source	(Optional) Specifies an IPv4 multicast source.
source-addr	IPv4 source address.
source-mask	(Optional) Mask for the group address.
source-prefix	(Optional) IPv4 multicast source prefix.
summary	(Optional) Displays the route counts.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about all the multicast FIB distribution routes:

```
switch(config)# show forwarding distribution multicast route
IPv4 Multicast Routing Table for table-id: 1
Total number of groups: 5
Legend:
   C = Control Route
```

Review Draft -- Cisco Confidential

```
    D = Drop Route
    G = Local Group (directly connected receivers)
    O = Drop on RPF Fail
    P = Punt to supervisor
    d = Decap Route

  (*, 224.0.0.0/4), RPF Interface: NULL, flags: D
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 0
    Null Outgoing Interface List

  (*, 224.0.0.0/24), RPF Interface: NULL, flags: CP
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 0
    Null Outgoing Interface List

  (*, 224.0.1.39/32), RPF Interface: NULL, flags: CP
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 0
    Null Outgoing Interface List

  (*, 224.0.1.40/32), RPF Interface: NULL, flags: CP
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 0
    Null Outgoing Interface List

  (*, 232.0.0.0/8), RPF Interface: NULL, flags: D
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 0
    Null Outgoing Interface List
switch#
```

Review Draft -- Cisco Confidential

show forwarding inconsistency

To display the results of the forwarding inconsistency checker, use the **show forwarding inconsistency** command.

show forwarding inconsistency [**ip** | **ipv4**] [**unicast**] **module** *slot* [**vrf** *vrf-name*]

Syntax Description

ip	(Optional) Displays the IPv4 forwarding inconsistency information.
ipv4	(Optional) Displays the IPv4 forwarding inconsistency information.
unicast	(Optional) Displays the forwarding inconsistency information for unicast routes
module *slot*	Displays inconsistency information for the module. The slot range depends on the hardware platform.
vrf *vrf-name*	(Optional) Displays inconsistency information for the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show forwarding inconsistency** command to display the results of the **test forwarding inconsistency** command.

Examples

This example shows how to display the forwarding inconsistency information for module 2:

```
switch# show forwarding inconsistency module 2
```

Related Commands

Command	Description
clear forwarding inconsistency	Clears the forwarding inconsistency checker.
test forwarding inconsistency	Triggers the forwarding inconsistency checker.

Review Draft -- Cisco Confidential

show forwarding multicast outgoing-interface-list

To display information about the multicast Forwarding Information Base (FIB) outgoing interface (OIF) list, use the **show forwarding multicast outgoing-interface-list** command.

show forwarding multicast outgoing-interface-list [*index*]

Syntax Description

index	(Optional) OIF list index. The OIF list index is from 1 to 65535.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the multicast FIB OIF list:

```
switch# show forwarding multicast outgoing-interface-list

  Outgoing Interface List Index: 1
  Reference Count: 1
    Ethernet1/5
switch#
```

Related Commands

Command	Description
clear ip igmp interface statistics	Clears the IGMP statistics for an interface.
ip igmp static-oif	Binds a multicast group to the outgoing interface (OIF).

Review Draft -- Cisco Confidential

show forwarding multicast route

To display information about the IPv4 Forwarding Information Base (FIB) multicast routes, use the **show forwarding multicast route** command.

show forwarding [**vrf** {*vrf-name* | **all**}] [**ip** | **ipv4**] **multicast route** {[**group** {*group-addr* [*group-mask*] | *group-prefix*} | **source** {*source-addr* [*source-mask*] | *source-prefix*} | **module** *num* | **vrf** {*vrf-name* | **all**}] | **summary** [**vrf** {*vrf-name* | **all**}]}

Syntax Description

vrf	(Optional) Displays information for a specified virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Displays information for all VRFs.
ip	(Optional) Specifies IPv4.
ipv4	(Optional) Specifies IPv4.
group	(Optional) Specifies an IPv4 multicast group address.
group-addr	IPv4 multicast group address.
group-mask	(Optional) IPv4 multicast group address mask.
group-prefix	(Optional) IPv4 multicast group prefix.
source	(Optional) Specifies an IPv4 multicast source address.
source-addr	IPv4 multicast source address.
source-mask	IPv4 multicast source address mask.
source-prefix	IPv4 multicast source prefix.
summary	Displays route counts.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the IPv4 multicast FIB routes:

```
switch# show forwarding multicast route

IPv4 Multicast Routing table table-id:1
Total number of groups: 1
```

Review Draft -- Cisco Confidential

```
Legend:
   C = Control Route
   D = Drop Route
   G = Local Group (directly connected receivers)
   O = Drop on RPF failure
   P = Punt to Supervisor
   W = Wildcard
   d = OTV Decap route

  (*, 230.0.0.0/32), RPF Interface: NULL, flags: DG
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 1
      Ethernet1/5 Outgoing Packets:0 Bytes:0
switch#
```

This example shows how to display the summary information about the IPv4 multicast FIB routes:

```
switch# show forwarding multicast route summary

IPv4 Multicast Routing Table for Context "default"
Total number of routes: 1
Total number of (*,G) routes: 1
Total number of (S,G) routes: 0
Total number of (*,G-prefix) routes: 0
Group count: 1
Prefix insert fail count: 9
switch#
```

Related Commands

Command	Description
clear ip mroute	Clears the multicast routing table.

Review Draft -- Cisco Confidential

show ip adjacency

To display adjacency information, use the **show ip adjacency** command.

show ip adjacency [*ip-addr* | *interface*] [**detail**] [**non-best**] [**statistics**] [**summary**] [**vrf** *vrf-name* | **all** | **default** | **management**]

Syntax Description

ip-addr	(Optional) IPv4 source address. The format is x.x.x.x.
interface	(Optional) Interface. Use *?* to determine the supported interface types.
detail	(Optional) Displays detailed adjacency information.
non-best	(Optional) Displays both the best and nonbest adjacency information.
statistics	(Optional) Displays adjacency statistics.
summary	(Optional) Displays a summary of the adjacency information.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Displays adjacency statistics for all VRF entries.
default	(Optional) Displays adjacency statistics for the default VRF.
management	(Optional) Displays adjacency statistics for the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The counter values in the output of **show ip adjacency** {**statistics** | **detail**} command are cleared after a supervisor module switchover.

Examples

This example shows how to display a summary of the adjacency information:

```
switch# show ip adjacency summary

IP Adjacency Table for VRF default
Total number of entries: 1
Address         MAC Address     Pref Source     Interface
2.2.2.100       000a.000a.000a  1    Static     Ethernet1/2
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show forwarding adjacency	Displays forwarding adjacency information.

Review Draft -- Cisco Confidential

show ip adjacency summary

To display the IP adjacency summary, use the **show ip adjacency summary** command.

show ip adjacency summary

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the IP adjacency summary:

```
switch# show ip adjacency summary
I
IP AM Table - Adjacency Summary

  Static  : 1
  Dynamic : 0
  Others  : 0
  Total   : 1

switch#
```

Related Commands

Command	Description
ip arp timeout	Configures ARP.

Review Draft -- Cisco Confidential

show ip fib

To display forwarding information, use the **show ip fib** command.

show ip fib {**adjacency** | **interfaces** | **route**} **module** *slot*

Syntax Description

adjacency	Displays the adjacency information.
interfaces	Displays the forwarding information for interfaces on a module.
route	Displays the forwarding information for routes on a module.
module *slot*	Displays information for the module. The slot range depends on the hardware platform.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show ip fib** command on the supervisor to view forwarding information on a module. Optionally, you can use the **attach module** command to attach to a module and use the **show ip fib** command on the module.

Examples

This example shows how to display the forwarding information for module 1:

```
switch# show ip fib route module 1

IPv4 routes for table default/base

------------------+------------------+----------------------
Prefix            | Next-hop         | Interface
------------------+------------------+----------------------
0.0.0.0/32          Drop               Null0
255.255.255.255/32  Receive            sup-eth1
switch#
```

Related Commands

Command	Description
show forwarding	Displays information about the FIB.

Review Draft -- Cisco Confidential

show ip fib distribution

To display forwarding distribution information, use the **show ip fib distribution** command.

show ip fib distribution [**clients** | **state**]

Syntax Description

clients	(Optional) Displays the forwarding distribution information for unicast clients.
state	(Optional) Displays the forwarding distribution state for unicast FIB.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the forwarding information for unicast clients:

```
switch# show ip fib distribution clients
```

Related Commands

Command	Description
show forwarding distribution	Displays distribution information about the FIB.

Review Draft -- Cisco Confidential

show ip load-sharing

To display IP load sharing information, use the **show ip load-sharing** command.

show ip load-sharing

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the IP load sharing information:

```
switch# show ip load-sharing
```

Related Commands

Command	Description
show ip load-sharing	Displays IP load sharing.

Review Draft -- Cisco Confidential

show ip process

To display formation about the IP process, use the **show ip process** command.

show ip process [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The *vrf-name* argument can be specified as any case-sensitive, alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows details about the IP process:

```
switch(config)# show ip process
VRF default
  VRF id is 1
  Base table id is 1
  Auto discard is disabled
  Auto discard is not added
  Auto Null broadcast is configured
  Auto Punt broadcast is configured
  Static discard is not configured
  Number of static default route configured is 0
  Number of ip unreachable configured is 0
  Iodlist: 73 74
  Local address list:  1.1.1.1          2.2.2.1          21.1.1.1
switch(config)#
```

Review Draft -- Cisco Confidential

show ip route

To display routes from the unicast Routing Information Base (RIB), use the **show ip route** command.

show ip route [**all** | *addr* | *hostname* | *prefix* | *route-type* | **interface** *type number* | **next-hop** *addr*]] [**vrf** *vrf-name*]

Syntax Description

all	(Optional) Displays all routes.
addr	(Optional) IPv4 address. The format is x.x.x.x.
hostname	Hostname. The *name* can be any case-sensitive, alphanumeric string up to 80 characters.
prefix	(Optional) IPv4 prefix. The format is x.x.x.x/length. The length range is from 1 to 32.
route-type	(Optional) Type of route. Use **?** to see the list of types.
interface *type number*	(Optional) Displays the routes for an interface. Use **?** to see the supported interfaces.
next-hop *addr*	(Optional) Displays routes with this next-hop address. The format is x.x.x.x.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the route table:

```
switch(config)# show ip route all
```

Related Commands

Command	Description
clear ip route	Clears entries in the route table.

Review Draft -- Cisco Confidential

show ip static-route

To display static routes from the unicast Routing Information Base (RIB), use the **show ip static-route** command.

show ip static-route [**vrf** {*vrf-name* | **all**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all virtual router contexts (VRF) name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the static routes:

```
switch(config)# show ip static-route
```

Related Commands

Command	Description
ip route	Configures a static route.

Review Draft -- Cisco Confidential

show routing

To display routing information, use the **show routing** command.

show routing [**ip** | **ipv4**] [*address* | *hostname* | *prefix* | *route-type* | **clients** | **hidden-nh interface** *type number* | **next-hop** *addr* | **recursive-next-hop** [*addr*]] [**vrf** *vrf-name*]

Syntax Description

ip	(Optional) Displays the routing information for the network.
ipv4	(Optional) Displays the routing information for the IPv4 network.
address	(Optional) IPv4 address. IPv4 address format is x.x.x.x.
hostname	Hostname. The *name* can be any case-sensitive, alphanumeric string up to 80 characters.
prefix	(Optional) IPv4 prefix. IPv4 prefix format is x.x.x.x/length.
route-type	(Optional) Type of route. Use **?** to see the list of types.
clients	(Optional) Displays the routing clients.
hidden-nh	(Optional) Displays hidden next-hop information.
interface *type number*	(Optional) Displays the routes for an interface. The interface can be one of the following: • **mgmt**—Management interface. The default management interface is 0. • **vlan**—VLAN interface. The VLAN interface number is from 1 to 4094.
next-hop *addr*	(Optional) Displays routes with this next-hop address. The format is x.x.x.x.
recursive next-hop *addr*	(Optional) Displays routes with this recursive next-hop address. The format is x.x.x.x.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The VRF can be one of the following: • *vrf-name*—VRF name. The name can be any case-sensitive, alphanumeric string up to 32 characters. • **all**—Specifies all VRFs. • **default**—Specifies the default VRF. • **management**—Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the route table:

Review Draft -- Cisco Confidential

```
switch(config)# show ip routing
```

Related Commands

Command	Description
clear ip route	Clears entries in the route table.

Review Draft -- Cisco Confidential

show routing memory estimate

To display an estimate of routing memory requirements, use the **show routing memory estimate** command.

show routing memory estimate [**routes** *num-routes* **next-hops** *num-hop-addresses*]

Syntax Description

routes	(Optional) Specifies the unicast Routing Information Base (RIB) memory estimate for the number of routes.
num-routes	Number of routes. The range is from 1000 to 1,000,000.
next-hops	(Optional) Specifies the unicast RIB memory estimate for the number of next hops per route.
num-hop-addresses	Number of next-hop addresses per route. The range is from 1 to 16.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **show routing memory estimate** command to estimate the memory required for a selected number of routes and number of next-hop addresses per route.

Examples

This example shows how to display the route table:

```
switch# show routing memory estimate routes 1000 next-hops 1
Shared memory estimates:
  Current max     32 MB;  27495 routes with 16 nhs
          in-use   1 MB;     11 routes with  1 nhs (average)
  Configured max  32 MB;  27495 routes with 16 nhs
  Estimate         0 MB;   1000 routes with  1 nhs
```

Review Draft -- Cisco Confidential

show routing hash

To display the route selected for a particular source and destination address, use the **show routing hash** command.

show routing hash *source-addr dest-addr* [*source-port dest-port*]] [**vrf** *vrf-name*]

Syntax Description

source-addr	Source IPv4 address. IPv4 address format is x.x.x.x.
dest-addr	Destination IPv4 address. IPv4 address format is x.x.x.x.
source-port	(Optional) Source port. The range is from 1 to 65535.
dest-port	(Optional) Destination port. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the route selected to reach 30.0.0.2 from 10.0.0.5:

```
switch# show routing hash  10.0.0.5 30.0.0.2
```

Related Commands

Command	Description
clear ip route	Clears entries in the route table.

Review Draft -- Cisco Confidential

show sockets client

To display information about the sockets clients, use the **show sockets client** command.

show sockets client [**pid** *id*] [**raw** | **tcp** | **udp**] [**detail**]

Syntax Description

pid *id*	(Optional) Displays the socket client information for a specific process. The *id* range is from 1 to 65535.
raw	(Optional) Displays information about the raw client.
tcp	(Optional) Displays information about the TCP client.
udp	(Optional) Displays information about the UDP client.
detail	(Optional) Displays information about the detailed client.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the UDP socket client information:

```
switch# show sockets client udp

Total number of UDP clients: 9

client: syslogd, pid: 4367, sockets: 2

client: ntpd, pid: 4602, sockets: 3

client: ntp, pid: 4591, sockets: 2

client: radiusd, pid: 4586, sockets: 2

client: dhcp_snoop, pid: 5260, sockets: 1

client: pim, pid: 5296, sockets: 1

client: mcecm, pid: 5265, sockets: 1

client: snmpd, pid: 4609, sockets: 2

client: hsrp_engine, pid: 9588, sockets: 2

Statistics: Cancels 12777, Cancel-unblocks 11257, Cancel-misses 0
            Select-drops 1520, Select-wakes 11257,
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear sockets statistics	Clears socket statistics.
show sockets connection	Displays information about the socket connection.
show sockets statistics	Displays information about the socket statistics.

Review Draft -- Cisco Confidential

show sockets connection

To display information about the sockets connection, use the **show sockets connection** command.

show sockets connection [**pid** *id*] [**local** *address* | **foreign** *address* | **raw** | **tcp** | **udp**] [**detail**]

Syntax Description

pid *id*	(Optional) Displays the socket client information for a specific process. the *id* range is from 1 to 65535.
local *address*	(Optional) Displays information about all the TCP connections with the specified local address. The *address* can be an IPv4 address.
foreign *address*	(Optional) Displays information about all the TCP connections with the specified foreign address. The *address* can be an IPv4 address.
raw	(Optional) Displays information about the raw client.
tcp	(Optional) Displays information about the TCP client.
udp	(Optional) Displays information about the UDP client.
detail	(Optional) Displays information about the detailed client.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the TCP socket connection information:

```
switch# show sockets connection tcp

Total number of tcp sockets: 4
Active connections (including servers)
Protocol State/       Recv-Q/   Local Address(port)/
         Context      Send-Q    Remote Address(port)
tcp6     LISTEN       0         *(22)
         Wildcard     0         *(*)

tcp6     LISTEN       0         *(23)
         Wildcard     0         *(*)

tcp      LISTEN       0         *(161)
         Wildcard     0         *(*)

tcp      ESTABLISHED  0         172.29.231.33(23)
         management   4         72.163.177.151(1559)


switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear sockets statistics	Clears the socket statistics.
show sockets client	Displays information about the socket client.
show sockets statistics	Displays the socket statistics.

Review Draft -- Cisco Confidential

show sockets statistics

To display the socket statistics, use the **show sockets statistics** command.

show sockets statistics [**all** | **raw** | **rawsum** | **tcp** | **tcpsum** | **udp** | **udpsum**]

Syntax Description

all	(Optional) Displays all the socket statistics.
raw	(Optional) Displays the socket statistics for the raw IPv4 protocol socket statistics.
rawsum	(Optional) Displays a summary of the socket statistics for the raw IPv4 protocol socket statistics.
tcp	(Optional) Displays the socket statistics for the TCP IPv4 protocol.
tcpsum	(Optional) Displays a summary of the socket statistics for the TCP IPv4 protocols.
udp	(Optional) Displays the socket statistics for the UDP IPv4 protocol.
udpsum	(Optional) Displays a summary of the socket statistics for the UDP IPv4 protocols.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the TCP socket statistics:

```
switch# show sockets statistics tcp
TCP v4 Received:
        11622 packets total
        0 checksum error, 0 bad offset, 0 too short, 0 MD5 error
        8782 packets (33566 bytes) in sequence
        0 duplicate packets (0 bytes)
        0 partially dup packets (0 bytes)
        0 out-of-order packets (0 bytes)
        0 packets (0 bytes) with data after window
        0 packets after close
        0 window probe packets, 0 window update packets
        2 duplicate ack packets, 0 ack packets with unsent data
        9349 ack packets (890960 bytes)
TCP v4 Sent:
        9543 total, 0 urgent packets
        3 control packets
        9492 data packets (890955 bytes)
        0 data packets (0 bytes) retransmitted
        48 ack only packets
        0 window probe packets, 0 window update packets
TCP v4:
0 connections initiated, 6 connections accepted, 6 connections established
6 connections closed (including 2 dropped, 0 embryonic dropped)
```

Review Draft -- Cisco Confidential

```
0 total rxmt timeout, 0 connections dropped in rxmt timeout
0 keepalive timeout, 0 keepalive probe, 0 connections dropped in keepalive
switch#
```

Related Commands

Command	Description
clear sockets statistics	Clears socket statistics.
show sockets client	Displays information about the socket client.
show sockets connection	Displays information about the socket connection.

Review Draft -- Cisco Confidential

T Commands

This chapter describes the Cisco NX-OS unicast Routing Information Base (RIB) and the Forwarding Information Base (FIB) commands that begin with T.

Review Draft -- Cisco Confidential

test forwarding distribution perf

To test the forwarding distribution performance of the Forwarding Information Base (FIB), use the **test forwarding distribution perf** command.

test forwarding distribution perf

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to test the forwarding distribution performance:

```
switch# test forwarding distribution perf
```

Related Commands

Command	Description
show forwarding distribution	Displays information about the FIB.

Review Draft -- Cisco Confidential

test forwarding inconsistency

To trigger the Layer 3 inconsistency checker for the Forwarding Information Base (FIB), use the **test forwarding inconsistency** command.

test forwarding inconsistency [**ip** | **ipv4**] [**unicast**] [**vrf** *vrf-name*] [**module** {*slot* | **all**}] [**stop**]

Syntax Description

ip	(Optional) Specifies the inconsistency check for IPv4 routes.
ipv4	(Optional) Specifies the inconsistency check for IPv4 routes.
unicast	(Optional) Specifies the inconsistency check for unicast routes.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) context name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
module	(Optional) Specifies the inconsistency check for one or more modules.
slot	Module number. The range depends on the platform.
all	(Optional) Specifies the inconsistency check for all modules.
stop	(Optional) Stops the inconsistency check.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to trigger the Layer 3 inconsistency checker for all modules:

```
switch# test forwarding inconsistency module all
```

This example shows how to stop the Layer 3 inconsistency checker for all modules:

```
switch# test forwarding inconsistency module all stop
```

Related Commands

Command	Description
clear forwarding inconsistency	Clears the FIB inconsistencies.
show forwarding inconsistency	Displays information about the FIB inconsistencies.

Review Draft -- Cisco Confidential

<I_Italic>Review Draft -- Cisco Confidential

PART 9

VRRP Commands

Review Draft -- Cisco Confidential

A Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands that begin with A.

Review Draft -- Cisco Confidential

address (VRRP)

To add a single, primary IP address to a virtual router, use the **address** command. To remove an IP address from a virtual router, use the **no** form of this command.

address *ip-address* [**secondary**]

no address [*ip-address* [**secondary**]]

Syntax Description

ip-address	Virtual router address (IPv4). This address should be in the same subnet as the interface IP address.
secondary	(Optional) Specifies a secondary virtual router address.

Command Default

None

Command Modes

VRRP configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can configure one virtual router IP address for a virtual router. If the configured IP address is the same as the interface IP address, this switch automatically owns the IP address. You can configure an IPv4 address only.

The master VRRP router drops the packets addressed to the virtual router's IP address because the virtual router is only intended as a next-hop router to forward packets. In NX-OS devices, some applications require that packets addressed to the virtual router's IP address be accepted and delivered. By using the **secondary** option to the virtual router IPv4 address, the VRRP router will accept these packets when it is the master.

This command does not require a license.

Examples

This example shows how to configure a virtual router IP address:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 250
switch(config-if-vrrp)# address 10.0.0.10
```

This example shows how to remove all the IP addresses (primary and secondary) using a single command:

Need new output[1]

```
switch(config-if-vrrp)# show running-config interface ethernet 9/10
```

1.

Review Draft -- Cisco Confidential

```
!Command: show running-config interface Ethernet9/10
!Time: Mon Apr 14 06:04:18 2008

version 5.0(3)N1(1)

interface Ethernet9/10
  vrrp 1
    address 10.10.10.1/24
  no shutdown

switch(config-if-vrrp)# no address
switch(config-if-vrrp)# show running-config interface ethernet 9/10

!Command: show running-config interface Ethernet1/5
!Time: Mon Apr 14 06:07:54 2008

version 5.0(3)N1(1)

interface Ethernet9/10
  no switchport
  vrrp 1
switch(config-if-vrrp)#
```

Related Commands

Command	Description
clear vrrp	Clears all the software counters for the specified virtual router.
show vrrp	Displays VRRP configuration information.
vrrp	Configures a VRRP group.

Review Draft -- Cisco Confidential

advertisement-interval (VRRP)

To specify the time interval between the advertisement packets that are being sent to other Virtual Router Redundancy Protocol (VRRP) routers in the same group, use the **advertisement-interval** command. To return to the default interval value of 1 second, use the **no** form of this command.

advertisement-interval *seconds*

no advertisement-interval [*seconds*]

Syntax Description

seconds	Number of seconds between advertisement frames being sent. For IPv4, the range is from 1 to 255 seconds.

Command Default

1 second

Command Modes

VRRP configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

VRRP advertisements communicate the priority and state of the virtual router master. The advertisements are encapsulated in IP packets and are sent to the IPv4 multicast address that is assigned to the VRRP group.

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA-assigned VRRP IP protocol number is 112.

Examples

This example shows how to specify an advertisement interval of 200 seconds for VRRP group 250:

```
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 250
switch(config-if-vrrp)# advertisement-interval 200
switch(config-if-vrrp)#
```

Related Commands

Command	Description
clear vrrp	Clears all the software counters for the specified virtual router.
show vrrp	Displays VRRP configuration information.
vrrp	Configures a VRRP group.

Review Draft -- Cisco Confidential

authentication (VRRP)

To configure an authentication for the Virtual Router Redundancy Protocol (VRRP), use the **authentication** command. To disable authentication, use the **no** form of this command.

authentication text *password*

no authentication [**text** *password*]

Syntax Description

text *password*	Selects to use simple text password of up to 8 alphanumeric characters.

Command Default

No authentication

Command Modes

VRRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to configure MD5 authentication for VRRP:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 250
switch(config-if-vrrp)# authentication text mypwasswd
switch(config-if-vrrp)#
```

Related Commands

Command	Description
clear vrrp	Clears all the software counters for the specified virtual router.
show vrrp	Displays VRRP configuration information.
vrrp	Configures a VRRP group.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands that begin with C.

Review Draft -- Cisco Confidential

clear ip interface statistics

To clear IP interface statistics, use the **clear ip interface statistics** command.

clear ip interface statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear the IP interface statistics:

```
switch# clear ip interface statistics
```

Related Commands

Command	Description
show ip interface	Displays IP interface information.

Review Draft -- Cisco Confidential

clear vrrp

To clear the Virtual Router Redundancy Protocol (VRRP) statistics, use the **clear vrrp** command.

clear vrrp vr *id* **interface** {**ethernet** *slot/port* | **port-channel** *number*[**.***sub_if_number*]}

Syntax Description

vr *id*	Clears VRRP statistics in a VRRP group on an interface. The range is from 1 to 255.
interface	Specifies an Ethernet or EthreChannel interface or a subinterface.
ethernet *slot/port*	Clears VRRP statistics on the Ethernet interface. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Clears VRRP statistics on the EtherChannel interface. The EtherChannel number is from 1 to 4096.
.*sub_if_number*	(Optional) Subinterface number. The range is from 1 to 4093.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to clear VRRP statistics from a specific Ethernet interface:

```
switch(config)# clear vrrp vr 1 interface ethernet 1/5
switch(config)#
```

Related Commands

Command	Description
feature vrrp	Enables the VRRP feature.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands that begin with F.

Review Draft -- Cisco Confidential

feature vrrp

To enable the Virtual Router Redundancy Protocol (VRRP), use the **feature vrrp** command. To disable VRRP, use the **no** form of this command.

feature vrrp

no feature vrrp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the VRRP feature before you can configure VRRP.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to enable the VRRP feature:

```
switch# configure terminal
switch(config)# feature vrrp
switch(config)#
```

This example shows how to disable the VRRP feature:

```
switch# configure terminal
switch(config)# no feature vrrp
switch(config)#
```

Related Commands

Command	Description
clear vrrp	Clears all the software counters for the specified virtual router.
show feature	Displays the status of features on a switch.
show vrrp	Displays VRRP configuration information.
vrrp	Configures a VRRP group on an interface.

Review Draft -- Cisco Confidential

P Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands that begin with P.

Review Draft -- Cisco Confidential

preempt (VRRP)

To enable a high-priority backup virtual router to preempt the low-priority master virtual router, use the **preempt** command. To disable a high-priority backup virtual router from preempting the low-priority master virtual router, use the **no** form of this command.

preempt

no preempt

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

VRRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a high-priority virtual router backup that has become available.

By default, a preemptive scheme is enabled. A backup high-priority virtual router that becomes available takes over for the backup virtual router that was elected to become the virtual router master. If you disable preemption, the backup virtual router that is elected to become the virtual router master remains the master until the original virtual router master recovers and becomes the master again.

Note This preemption does not apply to the primary IP address.

If the virtual IP address is also the IP address for the interface, then preemption is applied.

This command does not require a license.

Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Examples

This example shows how to enable the backup high-priority virtual router to preempt the low-priority master virtual router:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 250
switch(config-if-vrrp)# preempt
switch(config-if-vrrp)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear vrrp	Clears all the software counters for the specified virtual router.
show vrrp	Displays VRRP configuration information.
vrrp	Configures a VRRP group.

Review Draft -- Cisco Confidential

priority (VRRP)

To set the priority for the Virtual Router Redundancy Protocol (VRRP), use the **priority** command. To revert to the default value, use the **no** form of this command.

priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

no priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]

Syntax Description

level	Interface priority for a virtual router. The range of values is from 1 to 254. If this router is the owner of the IP addresses, then the value is automatically set to 254. The default is 100.
forwarding-threshold	(Optional) Sets the threshold used by a virtual port channel (vPC) to determine when to fail over to the vPC trunk.
lower *lower-value*	(Optional) Sets the low threshold value. The range is from 1 to 254. The default is 1.
upper *upper-value*	(Optional) Sets the upper threshold value. The range is from 1 to 254. The default is 254.

Command Default

The default value is 100. For switches whose interface IP address is the same as the primary virtual IP address, the default value is 254.

Command Modes

VRRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The priority determines whether or not a VRRP router functions as a virtual router backup, the order of ascendancy for the VRRP router to become a virtual router master if the virtual router master fails, the role that each VRRP router plays, and what happens if the virtual router master fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, then this router functions as a virtual router master.

By default, a preemptive scheme is enabled. A backup high-priority virtual router that becomes available takes over for the backup virtual router that was elected to become the virtual router master. If you disable preemption, then the backup virtual router that is elected to become the virtual router master remains the master until the original virtual router master recovers and becomes the master again.

This command does not require a license.

Examples

This example shows how to specify the priority for a virtual router:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
```

Review Draft -- Cisco Confidential

```
switch(config-if)# no switchport
switch(config-if)# vrrp 250
switch(config-if-vrrp)# priority 2
switch(config-if-vrrp)#
```

Related Commands

Command	Description
feature vrrp	Enables VRRP.
preempt	Enables preemption on the virtual router.
show vrrp	Displays VRRP configuration information.
shutdown (VRRP)	Disables the VRRP configuration.
vrrp	Configures a VRRP group.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

S Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands that begin with S.

Review Draft -- Cisco Confidential

shutdown (VRRP)

To disable a Virtual Router Redundancy Protocol (VRRP) configuration, use the **shutdown** command. To enable a VRRP configuration, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

VRRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Shut down the virtual router before configuring the virtual router parameters; you can only configure the virtual router after it is in the administrative shut down state. Enter the **no shutdown** command to update the virtual router state after completing configuration.

Examples

This example shows how to shut down a VRRP group:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# vrrp 45
switch(config-if-vrrp)# shutdown
switch(config-if-vrrp)# address 6.6.6.45
switch(config-if-vrrp)# no shutdown
switch(config-if-vrrp)#
```

Related Commands

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.
clear vrrp	Clears all the software counters for the specified virtual router.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) **show** commands.

Review Draft -- Cisco Confidential

show vrrp

To show information about the Virtual Router Redundancy Protocol (VRRP), use the **show vrrp** command.

show vrrp [**detail** | **statistics** | **summary**] [**interface** *if-number*] [**vr** *id*] [**backup** | **init** | **master**]

Syntax Description

detail	(Optional) Displays detailed information about VRRP.
statistics	(Optional) Displays VRRP statistics.
summary	(Optional) Displays the VRRP summary.
interface *if-number*	(Optional) Displays information about VRRP on an interface. Use **?** to see a list of supported interfaces.
vr *id*	(Optional) Displays information about VRRP for a group. The *id* range is from 1 to 255.
backup	(Optional) Displays information about VRRP groups in the backup state.
init	(Optional) Displays information about VRRP groups in the init state.
master	(Optional) Displays information about VRRP groups in the master state.

Command Default

Display information for all VRRP groups.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display information about VRRP:

```
switch(config)# show vrrp
      Interface  VR IpVersion Pri   Time Pre State   VR IP addr
------------------------------------------------------------------
    Ethernet1/5   1   IPV4    200  200 s  Y    Init    192.0.1.10

switch(config)#
```

This example shows how to display the detailed configuration information about VRRP:

```
switch(config)# show vrrp detail

Ethernet1/5 - Group 1 (IPV4)
     State is Init(Administratively down)
     Virtual IP address is 192.0.1.10
     Priority 200, Configured 200
     Forwarding threshold(for VPC), lower: 1 upper: 200
     Advertisement interval 200
     Preemption enabled
     Virtual MAC address is 0000.5e00.0101
     Master router is Unknown
```

Review Draft -- Cisco Confidential

```
switch(config)#
```

This example shows how to displayinformation about a specific virtual router:

```
switch# show vrrp vr 1
      Interface  VR IpVersion Pri   Time Pre State   VR IP addr
--------------------------------------------------------------------
    Ethernet1/5   1   IPV4    200  200 s  Y    Init    192.0.1.10
switch#
```

Table 1 describes the significant fields shown in the display.

Table 1 show vrrp Field Descriptions

Field	Description
Interface	Interface on which VRRP is configured.
VR	ID of the virtual router.
IPVersion	IP address on the interface.
Pri	Priority range of the virtual router.
Time	Checksum of the complete contents of the link state advertisement.
Pre	Preemption state of the virtual router.
State	VRRP group state. The state can be one of the following: • Init • Backup • Master
VR IP addr	Virtual IPv4 address for a VRRP group.

Related Commands

Command	Description
clear vrrp	Clears VRRP statistics.
feature vrrp	Enables the VRRP feature.
vrrp	Creates a virtual router group.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

T Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands that begin with T.

Review Draft -- Cisco Confidential

track (VRRP)

To modify the priority for a virtual router based on a tracked object, use the **track** command. To disable priority tracking for a virtual router, use the **no** form of this command.

track *object-number* [**decrement** *value*]

no track *object-number* [**decrement** *value*]

Syntax Description

object-number	Number for a configured tracked object. The range is from 1 to 500.
decrement *value*	(Optional) Decrements the VRRP priority if the tracked object is down. The range is from 1 to 254.

Command Default

None

Command Modes

VRRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **track (VRRP)** command to change the priority of the virtual router based on the state of a configured tracked object. Use the track command to configure the tracked object. When the tracked object is down, the priority reverts to the priority value for the virtual router. When the tracked object is up, the priority of the virtual router is restored to the original value.

This command does not require a license.

Examples

This example shows how to enable object tracking for a virtual router:

```
switch# configure terminal
switch(config)# track 33 ip route 192.0.2.0/24 reachability
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 250
switch(config-if-vrrp)# track 33 priority 2
switch(config-if-vrrp)#
```

Related Commandsl

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.

Review Draft -- Cisco Confidential

Command	Description
track interfave (VRRP)	Tracks the state of an interface and modifies the VRRP priority if that interface state goes down.
vrrp	Configures a VRRP group.

Review Draft -- Cisco Confidential

track interface (VRRP)

To track the priority for a virtual router based on an interface, use the **track interface** command. To disable priority tracking for a virtual router, use the **no** form of this command.

track interface {**ethernet** *slot/port* | **port-channel** *number*[**.***sub_if_number*]} **priority** *value*

no track interface {**ethernet** *slot/port* | **port-channel** *number*[**.***sub_if_number*]} **priority** *value*

Syntax Description

ethernet *slot/port*	Specifies the virtual router interface for which to track the priority. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the port-channel group for which to track priority. The range is from 1 to 4096
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.
priority *value*	Specifies the interface priority for a virtual router. The range of values is from 1 to 254. If this router is the owner of the IP addresses, the value is automatically set to 254.

Command Default

Disabled

Command Modes

VRRP configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **track** command to change the priority of the virtual router based on the state of another interface in the switch. When the tracked interface is down, the priority reverts to the priority value for the virtual router. When the tracked interface is up, the priority of the virtual router is restored to the interface state tracking value.

Note Interface state tracking will not be operational unless you enable preemption on the interface.

This command does not require a license.

Examples

This example shows how to enable interface state tracking for a virtual router:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 250
switch(config-if-vrrp)# track interface ethernet 2/2 priority 2
switch(config-if-vrrp)#
```

Review Draft -- Cisco Confidential

Related CommandsI

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.
track (VRRP)	Tracks an object to modify the VRRP priority.
vrrp	Configures a VRRP group.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

V Commands

This chapter describes the Cisco NX-OS Virtual Router Redundancy Protocol (VRRP) commands that begin with V.

Review Draft -- Cisco Confidential

vrrp

To create a Virtual Router Redundancy Protocol (VRRP) group on a particular Ethernet interface and assign a number to the VRRP group and enter VRRP configuration mode, use the **vrrp** command. To remove a VRRP group, use the **no** form of this command.

vrrp *number*

no vrrp *number*

Syntax Description

number	VRRP group number, which you can configure for a Gigabit Ethernet port, including the main interfaces and subinterfaces. The range is from 1 to 255.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can configure VRRP only if its state is disabled. Make sure that you configure at least one IP address before you attempt to enable a virtual router.

Examples

This example shows how to create a VRRP group:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 7
switch(config-if-vrrp)#
```

This example shows how to create a VRRP group and configure an IPv4 address for the group:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# vrrp 7
switch(config-if-vrrp)# address 10.0.0.10
switch(config-if-vrrp)# no shutdown
switch(config-if-vrrp)#
```

Related Commands

Command	Description
clear vrrp	Clears all the software counters for the specified virtual router.
feature vrrp	Enables VRRP.

Review Draft -- Cisco Confidential

Command	Description
address (VRRP)	Adds a primary or secondary IP address to a virtual router.
show vrrp	Displays VRRP configuration information.

Review Draft -- Cisco Confidential