



Send document comments to nexus7k-docfeedback@cisco.com



Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.2

August 2, 2010

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

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.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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

Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.2
© 2008–2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

New and Changed Information xxiii

Preface xxv

Audience xxv

Organization xxv

Document Conventions xxvi

Related Documentation xxvii

Obtaining Documentation and Submitting a Service Request xxviii

A Commands L3-1

address (VRRP) L3-1

address-family (BGP) L3-3

address-family (EIGRP) L3-6

address-family (IS-IS) L3-8

address-family (OSPFv3) L3-11

address-family (RIP) L3-12

advertise-map L3-13

advertisement-interval (VRRP) L3-15

aggregate-address L3-17

area authentication (OSPF) L3-20

area default-cost (OSPF) L3-22

area default-cost (OSPFv3) L3-23

area filter-list (OSPF) L3-24

area filter-list (OSPFv3) L3-26

area nssa (OSPF) L3-28

area nssa (OSPFv3) L3-30

area range (OSPF) L3-32

area range (OSPFv3) L3-33

area stub (OSPF) L3-34

area stub (OSPFv3) L3-35

area virtual-link (OSPF) L3-37

Send document comments to nexus7k-docfeedback@cisco.com

area virtual-link (OSPFv3) L3-39
authentication (GLBP) L3-41
authentication (HSRP) L3-43
authentication (OSPF virtual link) L3-45
authentication (VRRP) L3-47
authentication key-chain (EIGRP) L3-48
authentication key-chain (IS-IS) L3-50
authentication mode (EIGRP) L3-52
authentication-check L3-53
authentication-key (OSPF virtual link) L3-55
authentication-type L3-56
auto-cost (OSPF) L3-58
auto-cost (OSPFv3) L3-60
autonomous-system L3-62

B Commands L3-63

bestpath L3-63
L3-65

C Commands L3-67

clear bgp L3-68
clear bgp dampening L3-69
clear bgp flap-statistics L3-70
clear bgp policy statistics aggregate-address L3-71
clear bgp policy statistics dampening L3-72
clear bgp policy statistics neighbor L3-73
clear bgp policy statistics redistribute L3-74
clear forwarding route L3-76
clear forwarding inconsistency L3-77
clear hardware ip verify L3-78
clear hardware ip verify address L3-80
clear hardware ip verify length L3-82
clear ip adjacency statistics L3-84
clear ip arp L3-85
clear ip bgp L3-86
clear ip bgp dampening L3-87
clear ip bgp flap-statistics L3-88

Send document comments to nexus7k-docfeedback@cisco.com

clear ip eigrp accounting	L3-89
clear ip eigrp neighbors	L3-90
clear ip eigrp policy statistics redistribute	L3-92
clear ip eigrp policy statistics redistribute	L3-94
clear ip eigrp redistribution	L3-96
clear ip eigrp traffic	L3-97
clear ip interface statistics	L3-98
clear ip mbgp	L3-99
clear ip mbgp dampening	L3-100
clear ip mbgp flap-statistics	L3-101
clear ip ospf neighbor	L3-102
clear ip ospf policy statistics	L3-104
clear ip ospf redistribution	L3-106
clear ip ospf statistics	L3-107
clear ip ospf traffic	L3-108
clear ip rip policy statistics redistribute	L3-109
clear ip rip statistics	L3-111
clear ip route	L3-112
clear ip traffic	L3-113
clear ip wccp	L3-114
clear ipv6 adjacency statistics	L3-115
clear ipv6 eigrp accounting	L3-116
clear ipv6 eigrp neighbors	L3-117
clear ipv6 eigrp route-map statistics redistribute	L3-119
clear ipv6 eigrp redistribution	L3-121
clear ipv6 eigrp traffic	L3-122
clear ipv6 icmp interface statistics	L3-123
clear ipv6 nd interface statistics	L3-124
clear ipv6 neighbor	L3-125
clear ipv6 route	L3-126
clear ipv6 traffic	L3-127
clear isis adjacency	L3-128
clear isis ip route-map statistics redistribute	L3-129
clear isis redistribution	L3-131
clear isis route-map statistics distribute	L3-132

Send document comments to nexus7k-docfeedback@cisco.com

clear isis statistics **L3-134**
clear isis traffic **L3-135**
clear ospfv3 neighbor **L3-136**
clear ospfv3 policy statistics **L3-138**
clear ospfv3 statistics **L3-140**
clear ospfv3 traffic **L3-141**
clear route-map pbr-statistics **L3-142**
clear sockets statistics **L3-143**
clear vrrp **L3-144**
confederation **L3-145**
L3-145

D Commands L3-147

dead-interval (OSPF virtual link) **L3-147**
dead-interval (OSPFv3 virtual link) **L3-149**
default-information originate (EIGRP) **L3-151**
default-information originate (IS-IS) **L3-153**
default-information originate (OSPF) **L3-155**
default-information originate (OSPFv3) **L3-157**
default-information originate (RIP) **L3-159**
default-metric (EIGRP) **L3-160**
default-metric (OSPF) **L3-162**
default-metric (OSPFv3) **L3-164**
default-metric (RIP) **L3-166**
delay minimum **L3-168**
delay **L3-170**
distance (EIGRP) **L3-171**
distance (IS-IS) **L3-173**
distance (OSPF) **L3-174**
distance (OSPFv3) **L3-175**
distance (RIP) **L3-176**
distribute **L3-178**
L3-179

E Commands L3-181

ebgp multihop **L3-181**
eigrp graceful-restart **L3-183**

Send document comments to nexus7k-docfeedback@cisco.com

[eigrp log-neighbor-changes](#) L3-184
[eigrp log-neighbor-warnings](#) L3-185
[eigrp router-id](#) L3-187
[eigrp stub](#) L3-188
 L3-189

F Commands L3-191

[feature bgp](#) L3-191
[feature eigrp](#) L3-193
[feature glbp](#) L3-194
[feature hsrp](#) L3-196
[feature isis](#) L3-197
[feature ospf](#) L3-198
[feature ospfv3](#) L3-199
[feature pbr](#) L3-200
[feature rip](#) L3-201
[feature vrrp](#) L3-202
[feature wccp](#) L3-203
[flush-routes \(OSPF\)](#) L3-204
[flush-routes \(OSPFv3\)](#) L3-205
[forwarder preempt](#) L3-206
 L3-206

G Commands L3-207

[glbp](#) L3-207
[graceful-restart \(BGP\)](#) L3-209
[graceful-restart \(EIGRP\)](#) L3-211
[graceful-restart \(IS-IS\)](#) L3-212
[graceful-restart \(OSPF\)](#) L3-213
[graceful-restart \(OSPFv3\)](#) L3-214
[graceful-restart t3 manual](#) L3-215
 L3-215

H Commands L3-217

[hardware forwarding dynamic-allocation](#) L3-218
[hardware ip verify](#) L3-219
[hardware ip verify address](#) L3-221

Send document comments to nexus7k-docfeedback@cisco.com

hardware ip verify length **L3-223**
hardware ipv6 verify **L3-225**
hello-interval (OSPF virtual link) **L3-226**
hello-interval (OSPFv3 virtual link) **L3-228**
hostname dynamic **L3-229**
hsrp **L3-231**
hsrp timers extended-hold **L3-233**
 L3-234

I Commands L3-235

ip (GLBP) **L3-235**
ip (HSRP) **L3-237**
ip arp **L3-239**
ip arp gratuitous **L3-240**
ip as-path access-list **L3-241**
ip authentication key-chain eigrp **L3-243**
ip authentication mode eigrp **L3-244**
ip bandwidth eigrp **L3-245**
ip bandwidth-percent eigrp **L3-246**
ip community-list **L3-247**
ip delay eigrp **L3-251**
ip directed-broadcast **L3-252**
ip distribute-list eigrp **L3-254**
ip domain-list **L3-256**
ip domain-lookup **L3-258**
ip domain-name **L3-259**
ip eigrp shutdown **L3-261**
ip extcommunity-list **L3-262**
ip hello-interval eigrp **L3-265**
ip hold-time eigrp **L3-266**
ip host **L3-268**
ip load-sharing address **L3-269**
ip load-sharing per-packet **L3-271**
ip name-server **L3-273**
ip next-hop-self eigrp **L3-275**
ip offset-list eigrp **L3-276**

Send document comments to nexus7k-docfeedback@cisco.com

[ip ospf authentication](#) **L3-278**
[ip ospf authentication-key](#) **L3-280**
[ip ospf cost](#) **L3-282**
[ip ospf dead-interval](#) **L3-283**
[ip ospf hello-interval](#) **L3-285**
[ip ospf message-digest-key](#) **L3-286**
[ip ospf mtu-ignore](#) **L3-287**
[ip ospf network](#) **L3-288**
[ip ospf passive-interface](#) **L3-289**
[ip ospf priority](#) **L3-290**
[ip ospf retransmit-interval](#) **L3-292**
[ip ospf shutdown](#) **L3-293**
[ip ospf transmit-delay](#) **L3-294**
[ip passive-interface eigrp](#) **L3-295**
[ip policy route-map](#) **L3-296**
[ip port-unreachable](#) **L3-298**
[ip prefix-list](#) **L3-299**
[ip prefix-list description](#) **L3-301**
[ip proxy-arp](#) **L3-302**
[ip rip authentication key-chain](#) **L3-303**
[ip rip authentication mode](#) **L3-304**
[ip rip metric-offset](#) **L3-305**
[ip rip offset-list](#) **L3-306**
[ip rip passive-interface](#) **L3-307**
[ip rip poison-reverse](#) **L3-308**
[ip rip route-filter](#) **L3-309**
[ip rip summary-address](#) **L3-310**
[ip route](#) **L3-311**
[ip router eigrp](#) **L3-313**
[ip router ospf area](#) **L3-314**
[ip router ospf multi-area](#) **L3-315**
[ip source-route](#) **L3-316**
[ip split-horizon eigrp](#) **L3-317**
[ip summary-address eigrp](#) **L3-318**
[ip wccp](#) **L3-320**

Send document comments to nexus7k-docfeedback@cisco.com

ip wccp redirect	L3-322
ip wccp redirect exclude in	L3-324
ip unreachable	L3-326
ipv6 address	L3-327
ipv6 authentication key-chain eigrp	L3-329
ipv6 authentication mode eigrp	L3-331
ipv6 bandwidth eigrp	L3-332
ipv6 bandwidth-percent eigrp	L3-333
ipv6 delay eigrp	L3-334
ipv6 distribute-list eigrp	L3-335
ipv6 eigrp shutdown	L3-337
ipv6 hello-interval eigrp	L3-338
ipv6 hold-time eigrp	L3-339
ipv6 host	L3-341
ipv6 nd hop-limit	L3-342
ipv6 nd managed-config-flag	L3-343
ipv6 nd mtu	L3-344
ipv6 nd ns-interval	L3-345
ipv6 nd other-config-flag	L3-346
ipv6 nd ra-interval	L3-347
ipv6 nd ra-lifetime	L3-348
ipv6 nd reachable-time	L3-349
ipv6 nd redirects	L3-350
ipv6 nd retrans-timer	L3-351
ipv6 nd suppress-ra	L3-352
ipv6 neighbor	L3-353
ipv6 next-hop-self eigrp	L3-355
ipv6 offset-list eigrp	L3-356
ipv6 passive-interface eigrp	L3-358
ipv6 policy route-map	L3-359
ipv6 prefix-list	L3-361
ipv6 prefix-list description	L3-363
ipv6 route	L3-364
ipv6 router eigrp	L3-366
ipv6 router ospfv3 area	L3-367

Send document comments to nexus7k-docfeedback@cisco.com

[ipv6 router ospfv3 multi-area](#) L3-368

[ipv6 split-horizon eigrp](#) L3-369

[ipv6 summary-address eigrp](#) L3-370

[ipv6 unreachable](#) L3-371

[is-type](#) L3-372

[isis authentication key-chain](#) L3-374

[isis authentication-check](#) L3-376

[isis authentication-type](#) L3-378

[isis circuit-type](#) L3-380

[isis csnp-interval](#) L3-382

[isis hello padding](#) L3-384

[isis hello-interval](#) L3-386

[isis hello-multiplier](#) L3-388

[isis lsp-interval](#) L3-390

[isis mesh-group](#) L3-391

[isis metric](#) L3-393

[isis passive](#) L3-395

[isis priority](#) L3-396

L Commands L3-399

[load-balancing](#) L3-399

[local-as](#) L3-401

[log-adjacency-changes \(EIGRP\)](#) L3-402

[log-adjacency-changes \(IS-IS\)](#) L3-403

[log-adjacency-changes \(OSPF\)](#) L3-404

[log-adjacency-changes \(OSPFv3\)](#) L3-405

[log-neighbor-warnings](#) L3-406

[low-memory exempt](#) L3-407

[lsp-gen-interval](#) L3-408

[lsp-mtu](#) L3-410

M Commands L3-411

[match as-number](#) L3-412

[match as-path](#) L3-414

[match community](#) L3-416

[match extcommunity](#) L3-418

[match interface](#) L3-420

Send document comments to nexus7k-docfeedback@cisco.com

[match ip address](#) **L3-422**
[match ip multicast](#) **L3-425**
[match ip next-hop prefix-list](#) **L3-428**
[match ip route-source prefix-list](#) **L3-430**
[match ipv6 address](#) **L3-432**
[match ipv6 multicast](#) **L3-435**
[match ipv6 next-hop prefix-list](#) **L3-438**
[match ipv6 route-source prefix-list](#) **L3-440**
[match length](#) **L3-442**
[match route-type](#) **L3-444**
[match tag](#) **L3-447**
[max-metric router-lsa \(OSPF\)](#) **L3-449**
[max-lsp-lifetime](#) **L3-451**
[maxas-limit](#) **L3-452**
[maximum-paths \(BGP\)](#) **L3-453**
[maximum-paths \(EIGRP\)](#) **L3-454**
[maximum-paths \(IS-IS\)](#) **L3-455**
[maximum-paths \(RIP\)](#) **L3-456**
[maximum-paths \(OSPF\)](#) **L3-457**
[maximum-paths \(OSPFv3\)](#) **L3-458**
[maximum-prefix](#) **L3-459**
[message-digest-key \(OSPF virtual link\)](#) **L3-461**
[metric maximum-hops](#) **L3-462**
[metric weights](#) **L3-463**
[metric-style transition](#) **L3-465**

N Commands **L3-467**

[neighbor](#) **L3-468**
[net](#) **L3-471**
[network](#) **L3-473**
[nexthop route-map](#) **L3-474**
[nexthop trigger-delay](#) **L3-476**

O Commands **L3-479**

[object](#) **L3-479**
[ospfv3 cost](#) **L3-481**
[ospfv3 dead-interval](#) **L3-482**

Send document comments to nexus7k-docfeedback@cisco.com

ospfv3 hello-interval **L3-484**
 ospfv3 mtu-ignore **L3-485**
 ospfv3 network **L3-486**
 ospfv3 passive-interface **L3-487**
 ospfv3 priority **L3-488**
 ospfv3 retransmit-interval **L3-490**
 ospfv3 shutdown **L3-491**
 ospfv3 transmit-delay **L3-492**

P Commands L3-493

platform ip verify **L3-494**
 platform ip verify address **L3-496**
 platform ip verify length **L3-498**
 platform ipv6 verify **L3-500**
 policy statistics enable (OSPF) **L3-502**
 policy statistics enable (OSPFv3) **L3-503**
 preempt (GLBP) **L3-504**
 preempt (HSRP) **L3-506**
 preempt (VRRP) **L3-508**
 priority (GLBP) **L3-510**
 priority (HSRP) **L3-511**
 priority (VRRP) **L3-513**
 protocol shutdown (OSPF) **L3-515**
 protocol shutdown (OSPFv3) **L3-516**

R Commands L3-517

redistribute (BGP) **L3-518**
 redistribute (EIGRP) **L3-520**
 redistribute (IS-IS) **L3-522**
 redistribute (OSPF) **L3-524**
 redistribute (OSPFv3) **L3-526**
 redistribute (RIP) **L3-528**
 redistribute maximum-prefix **L3-530**
 redistribute maximum-prefix (EIGRP) **L3-532**
 redistribute maximum-prefix (IS-IS) **L3-534**
 reference-bandwidth **L3-536**
 remote-as **L3-538**

Send document comments to nexus7k-docfeedback@cisco.com

[retransmit-interval \(OSPF virtual link\)](#) L3-540
[retransmit-interval \(OSPFv3 virtual link\)](#) L3-541
[route-map](#) L3-542
[route-map pbr-statistics](#) L3-548
[router bgp](#) L3-549
[router eigrp](#) L3-552
[router isis](#) L3-553
[router ospf](#) L3-554
[router ospfv3](#) L3-555
[router rip](#) L3-556
[router-id \(EIGRP\)](#) L3-557
[router-id \(OSPF\)](#) L3-558
[router-id \(OSPFv3\)](#) L3-559
[routing-context vrf](#) L3-560

S Commands L3-561

[set as-path](#) L3-561
[set comm-list delete](#) L3-564
[set community](#) L3-566
[set dampening](#) L3-569
[set etxcommunity](#) L3-571
[set extcomm-list delete](#) L3-573
[set forwarding-address](#) L3-575
[set ip default next-hop](#) L3-577
[set ip next-hop](#) L3-580
[set ipv6 default next-hop](#) L3-582
[set ipv6 next-hop](#) L3-585
[set level](#) L3-587
[set local-preference](#) L3-589
[set metric](#) L3-591
[set metric-type](#) L3-593
[set origin](#) L3-595
[set tag](#) L3-597
[set vrf](#) L3-599
[set weight](#) L3-601
[set-attached-bit](#) L3-603

Send document comments to nexus7k-docfeedback@cisco.com

[set-overload-bit](#) **L3-604**
[shutdown \(BGP\)](#) **L3-606**
[shutdown \(EIGRP\)](#) **L3-607**
[shutdown \(IS-IS\)](#) **L3-608**
[shutdown \(OSPF\)](#) **L3-609**
[shutdown \(OSPFv3\)](#) **L3-610**
[shutdown \(VRRP\)](#) **L3-611**
[spf-interval](#) **L3-613**
[stub](#) **L3-615**
[summary-address](#) **L3-617**
[summary-address \(OSPF\)](#) **L3-619**
[summary-address \(OSPFv3\)](#) **L3-621**
[suppress-inactive](#) **L3-623**

Show Commands **L3-625**

[show bgp](#) **L3-626**
[show bgp community](#) **L3-628**
[show bgp community-list](#) **L3-630**
[show bgp extcommunity](#) **L3-632**
[show bgp extcommunity-list](#) **L3-634**
[show bgp neighbors](#) **L3-636**
[show bgp sessions](#) **L3-638**
[show forwarding](#) **L3-639**
[show forwarding distribution](#) **L3-641**
[show forwarding inconsistency](#) **L3-642**
[show glbp](#) **L3-644**
[show glbp capability](#) **L3-650**
[show hardware forwarding dynamic-allocation status](#) **L3-652**
[show hardware forwarding ip verify](#) **L3-654**
[show hsrp](#) **L3-656**
[show hsrp delay](#) **L3-658**
[show hsrp summary](#) **L3-659**
[show ip adjacency](#) **L3-661**
[show ip arp](#) **L3-663**
[show ip as-path-access-list](#) **L3-665**
[show ip bgp](#) **L3-666**

Send document comments to nexus7k-docfeedback@cisco.com

show ip bgp community-list	L3-668
show ip bgp dampening	L3-670
show ip bgp extcommunity	L3-672
show ip bgp extcommunity-list	L3-673
show ip bgp filter-list	L3-674
show ip bgp flap-statistics	L3-675
show ip bgp history-paths	L3-676
show ip bgp neighbors	L3-677
show ip bgp nexthop	L3-679
show ip bgp nexthop-database	L3-680
show ip bgp peer-policy	L3-681
show ip bgp peer-session	L3-682
show ip bgp peer-template	L3-683
show ip bgp prefix-list	L3-685
show ip client	L3-686
show ip community-list	L3-687
show ip eigrp	L3-688
show ip eigrp accounting	L3-690
show ip eigrp interfaces	L3-692
show ip eigrp neighbors	L3-694
show ip eigrp policy statistics	L3-697
show ip eigrp route-map statistics	L3-699
show ip eigrp topology	L3-701
show ip eigrp traffic	L3-705
show ip fib	L3-707
show ip fib distribution	L3-708
show ip interface	L3-709
show ip load-sharing	L3-711
show ip mbgp	L3-712
show ip mbgp community	L3-714
show ip mbgp community-list	L3-715
show ip mbgp dampening	L3-716
show ip mbgp extcommunity	L3-718
show ip mbgp extcommunity-list	L3-719
show ip mbgp filter-list	L3-720

Send document comments to nexus7k-docfeedback@cisco.com

[show ip mbgp flap-statistics](#) **L3-721**
[show ip mbgp history-paths](#) **L3-722**
[show ip mbgp neighbors](#) **L3-723**
[show ip mbgp nexthop](#) **L3-725**
[show ip mbgp nexthop-database](#) **L3-726**
[show ip mbgp prefix-list](#) **L3-727**
[show ip ospf](#) **L3-728**
[show ip ospf border-routers](#) **L3-730**
[show ip ospf database](#) **L3-732**
[show ip ospf interface](#) **L3-738**
[show ip ospf lsa-content-changed-list](#) **L3-740**
[show ip ospf memory](#) **L3-742**
[show ip ospf neighbors](#) **L3-744**
[show ip ospf policy statistics area](#) **L3-747**
[show ip ospf policy statistics redistribute](#) **L3-748**
[show ip ospf request-list](#) **L3-750**
[show ip ospf retransmission-list](#) **L3-752**
[show ip ospf routes](#) **L3-754**
[show ip ospf statistics](#) **L3-756**
[show ip ospf summary-address](#) **L3-758**
[show ip ospf traffic](#) **L3-760**
[show ip ospf virtual-links](#) **L3-762**
[show ip policy](#) **L3-764**
[show ip prefix-list](#) **L3-765**
[show ip process](#) **L3-766**
[show ip rip](#) **L3-767**
[show ip rip interface](#) **L3-769**
[show ip rip neighbor](#) **L3-771**
[show ip rip policy statistics](#) **L3-773**
[show ip rip route](#) **L3-775**
[show ip rip statistics](#) **L3-777**
[show ip route](#) **L3-779**
[show ip static-route](#) **L3-781**
[show ip traffic](#) **L3-782**
[show ip wccp](#) **L3-784**

Send document comments to nexus7k-docfeedback@cisco.com

[show ipv6 adjacency](#) **L3-788**
[show ipv6 bgp](#) **L3-790**
[show ipv6 bgp community](#) **L3-792**
[show ipv6 bgp community-list](#) **L3-793**
[show ipv6 bgp dampening](#) **L3-794**
[show ipv6 bgp extcommunity-list](#) **L3-795**
[show ipv6 bgp filter-list](#) **L3-796**
[show ipv6 bgp flap-statistics](#) **L3-797**
[show ipv6 bgp history-paths](#) **L3-798**
[show ipv6 bgp neighbors](#) **L3-799**
[show ipv6 bgp nexthop](#) **L3-801**
[show ipv6 bgp nexthop-database](#) **L3-802**
[show ipv6 bgp prefix-list](#) **L3-803**
[show ipv6 client](#) **L3-804**
[show ipv6 eigrp](#) **L3-805**
[show ipv6 eigrp accounting](#) **L3-806**
[show ipv6 eigrp interfaces](#) **L3-808**
[show ipv6 eigrp neighbors](#) **L3-810**
[show ipv6 eigrp route-map statistics](#) **L3-813**
[show ipv6 eigrp topology](#) **L3-815**
[show ipv6 eigrp traffic](#) **L3-817**
[show ipv6 fragments](#) **L3-819**
[show ipv6 icmp interface](#) **L3-820**
[show ipv6 interface](#) **L3-821**
[show ipv6 mbgp](#) **L3-823**
[show ipv6 mbgp community](#) **L3-824**
[show ipv6 mbgp community-list](#) **L3-825**
[show ipv6 mbgp neighbors](#) **L3-826**
[show ipv6 nd interface](#) **L3-828**
[show ipv6 neighbor](#) **L3-830**
[show ipv6 policy](#) **L3-832**
[show ipv6 prefix-list](#) **L3-833**
[show ipv6 process](#) **L3-834**
[show ipv6 route](#) **L3-835**
[show ipv6 routers](#) **L3-837**

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 static-route	L3-838
show ipv6 traffic	L3-839
show isis adjacency	L3-841
show isis database	L3-843
show isis hostname	L3-845
show isis interface	L3-846
show isis ip route-map statistics redistribute	L3-848
show isis mesh-group	L3-850
show isis protocol	L3-851
show isis redistribute route	L3-853
show isis route	L3-855
show isis route-map statistics distribute	L3-858
show isis rrm	L3-860
show isis spf-log	L3-862
show isis srm	L3-864
show isis ssn	L3-866
show isis statistics	L3-868
show isis summary-address	L3-870
show isis traffic	L3-872
show ospfv3	L3-874
show ospfv3 border-routers	L3-876
show ospfv3 database	L3-878
show ospfv3 interface	L3-885
show ospfv3 memory	L3-887
show ospfv3 neighbors	L3-889
show ospfv3 policy statistics area	L3-891
show ospfv3 policy statistics redistribute	L3-892
show ospfv3 request-list	L3-894
show ospfv3 retransmission-list	L3-896
show ospfv3 routes	L3-898
show ospfv3 statistics	L3-900
show ospfv3 summary-address	L3-902
show ospfv3 traffic	L3-904
show ospfv3 virtual-links	L3-906
show routing	L3-908

Send document comments to nexus7k-docfeedback@cisco.com

[show routing memory estimate](#) L3-910

[show routing-context](#) L3-911

[show routing hash](#) L3-912

[show sockets client](#) L3-913

[show sockets connection](#) L3-915

[show sockets statistics](#) L3-917

[show track](#) L3-919

[show vrrp](#) L3-921

T Commands L3-923

[template \(BGP\)](#) L3-923

[test forwarding distribution perf](#) L3-930

[test forwarding inconsistency](#) L3-931

[threshold percentage](#) L3-933

[threshold weight](#) L3-935

[timers \(GLBP\)](#) L3-937

[timers active-time](#) L3-939

[timers basic](#) L3-940

[timers lsa-arrival \(OSPF\)](#) L3-942

[timers lsa-arrival \(OSPFv3\)](#) L3-944

[timers lsa-group-pacing \(OSPF\)](#) L3-946

[timers lsa-group-pacing \(OSPFv3\)](#) L3-948

[timers nsf converge](#) L3-950

[timers nsf route-hold](#) L3-951

[timers nsf signal](#) L3-952

[timers redirect](#) L3-953

[timers throttle lsa \(OSPF\)](#) L3-955

[timers throttle lsa \(OSPFv3\)](#) L3-957

[timers throttle spf \(OSPF\)](#) L3-959

[timers throttle spf \(OSPFv3\)](#) L3-960

[track \(VRRP\)](#) L3-961

[track interface](#) L3-963

[track interface\(VRRP\)](#) L3-965

[track ip route](#) L3-967

[track ipv6 route](#) L3-969

[track list](#) L3-971

Send document comments to nexus7k-docfeedback@cisco.com

[transmit-delay \(OSPF virtual link\)](#) **L3-973**

[transmit-delay \(OSPFv3 virtual link\)](#) **L3-974**

V Commands **L3-975**

[vrf](#) **L3-976**

[vrf context](#) **L3-979**

[vrf member](#) **L3-981**

[vrrp](#) **L3-982**

W Commands **L3-985**

[weighting](#) **L3-985**

[weighting track](#) **L3-987**

[wide-metric-only](#) **L3-989**

Send document comments to nexus7k-docfeedback@cisco.com



New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.2*. The latest version of this document is available at the following Cisco website:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/unicast/command/reference/unicast_cr.html

To check for additional information about Cisco NX-OS Release 4.2, see the *Cisco NX-OS Release Notes* available at the following Cisco website:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/release/notes/42_nx-os_release_note.html

Table 1 summarizes the new and changed features for the *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.2*, and tells you where they are documented.

Table 1 **New and Changed Features for Release 4.2**

Feature	Description	Changed in Release	Where Documented
BGP	Added advertise-map , nexthop trigger-delay , nexthop route-map , low-memory exempt and extended community commands.	4.2(1)	A Commands L Commands N Commands Show Commands
EIGRP, IS-IS	Added redistribute maximum-prefix commands.	4.2(1)	L Commands
OSPF	Added ip router ospf multi-area , ipv6 router ospfv3 multi-area , and redistribute maximum-prefix commands.	4.2(1)	I Commands L Commands
Route Policy Manager	Added ip extcommunity , match extcommunity , set extcommunity , and set excomm-delete commands.	4.2(1)	I Commands M Commands S Commands
WCCP	Added WCCPv2 commands.	4.2(1)	C Commands I Commands Show Commands

Send document comments to nexus7k-docfeedback@cisco.com



Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.2*. It also provides information on how to obtain related documentation.

This chapter includes the following sections:

- [Audience, page xxv](#)
- [Organization, page xxv](#)
- [Document Conventions, page xxvi](#)
- [Related Documentation, page xxvii](#)
- [Obtaining Documentation and Submitting a Service Request, page xxviii](#)

Audience

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

Organization

This reference is organized as follows:

Chapter and Title	Description
A Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter A.
B Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter B.
C Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter C.
D Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter D.
E Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter E.

Send document comments to nexus7k-docfeedback@cisco.com

Chapter and Title	Description
F Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter F.
G Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter G.
H Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter H.
I Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter I.
L Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter L.
M Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter M.
N Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter N.
O Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter O.
P Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter P.
R Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter R.
S Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter S, except for show commands.
Show Commands	Describes the Cisco NX-OS unicast routing show commands.
T Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter T.
V Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter V.
W Commands	Describes the Cisco NX-OS unicast routing commands that begin with the letter W.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
[]	Elements in square brackets are optional.
[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.

Send document comments to nexus7k-docfeedback@cisco.com

Screen examples use these conventions:

<code>screen font</code>	Terminal sessions and information that the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen font</i>	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.



Tip

Means *the following information will help you solve a problem*.

Related Documentation

[Cisco NX-OS](#) includes the following documents:

Release Notes

Cisco Nexus 7000 Series NX-OS Release Notes, Release 4.21

NX-OS Configuration Guides

Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 4.2

Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2

Send document comments to nexus7k-docfeedback@cisco.com

Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2

Cisco Nexus 7000 Series NX-OS XML Management Interface User Guide, Release 4.2

Cisco MDS 9000 Family and Nexus 7000 Series NX-OS System Messages Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS MIB Quick Reference

NX-OS Command References

Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 4.2

Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.12

Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 4.2

Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 4.2

Other Software Document

Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 4.x

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, at:

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

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



A Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter A.

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
```

Syntax Description	<i>ip-address</i>	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.

Defaults	None

Command Modes	VRRP configuration mode

SupportedUserRoles	network-admin VDC administrator

Command History	Release	Modified
	4.0(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.

Send document comments to nexus7k-docfeedback@cisco.com

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)# 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:

```
switch(config-if-vrrp)# show run interface ethernet 9/10
version 4.0(1)
```

```
interface Ethernet9/10
  vrrp 1
    address 10.10.10.10
    address 10.10.10.11 secondary
  ip address 10.10.10.1/24
  no shutdown
```

```
switch(config-if-vrrp)# no address
switch(config-if-vrrp)# sh run int e9/10
version 4.0(1)
```

```
interface Ethernet9/10
  vrrp 1
  ip address 10.10.10.1/24
  no shutdown
```

```
switch(config-if-vrrp)#
```

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.
clear vrrp	Clears all the software counters for the specified virtual router.

Send document comments to nexus7k-docfeedback@cisco.com

address-family (BGP)

To enter the address family mode or a 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 | ipv6} {multicast | unicast}

no address-family {ipv4 | ipv6} {multicast | unicast}

Syntax Description

ipv4	Specifies the IPv4 address family.
ipv6	Specifies the IPv6 address family.
multicast	Specifies multicast address support.
unicast	Specifies unicast address support.

Command Default

This command has no default settings.

Command Modes

Router configuration
Neighbor configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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. IPv6 neighbor sessions support IPv6 unicast and multicast address families.

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



Note

This applies to IPv4 multicast or unicast and IPv6 multicast or unicast.

- **suppress-inactive**—Advertise only active routes to peer. See the **suppress-inactive** command for additional information.

Send document comments to nexus7k-docfeedback@cisco.com

- **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.
- **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.

- **default-originate**—Originates a default toward this peer.
- **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.

Send document comments to nexus7k-docfeedback@cisco.com

- **network**—Configures an IP prefix to advertise. See the **network** command for additional information.
- **no**—Negates a command or set its defaults
- **redistribute**—Enables the redistribution of routes learned by other protocols into BGP. Redistribution is supported for both IPv4 and IPv6 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.
 - **isis src-protocol route-map name**—Specifies ISO IS-IS routes.
 - **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.

This command requires the 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)#
```

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

Related Commands

Command	Description
aggregate-address	Configures BGP summary addresses.
client-to-client	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.
redistribute (BGP)	Configures route redistribution for BGP.
timers (BGP)	Configures the BGP timers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

address-family (EIGRP)

To configure an address family for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **address-family** command in router configuration mode.

address-family {ipv4 | ipv6} unicast

Syntax Description	ipv4	Specifies the IPv4 address family.
	ipv6	Specifies the IPv6 address family.
	unicast	Specifies unicast address support.

Defaults	None

Command Modes	Router configuration Address family configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	The ipv6 keyword was added.

Usage Guidelines	This command requires the Enterprise license.

Examples	The following 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
```

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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
router-id	Configures the router ID.
timers	Configures the EIGRP timers.

Send document comments to nexus7k-docfeedback@cisco.com

address-family (IS-IS)

To enter the address family mode or a VRF address-family mode and configure submode commands for the Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS), 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 unicast

no address-family ipv4 unicast

Syntax Description	ipv4	Specifies the IPv4 address family.
	unicast	Specifies unicast address support.

Command Default	None

Command Modes	Router configuration VRF configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the address-family command to enter various address family configuration modes while configuring IS-IS routing. When you enter the address-family command from configuration mode, you enable the address family and enter global address family configuration mode. The prompt changes to <code>switch(config-router-af)#</code> .

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 address families. .

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

- **adjacency-check**—Allows Intermediate System-to-Intermediate System (IS-IS) IPv4 protocol-support consistency checks to be performed on hello packets. To disable consistency checks on hello packets, use the **no** form of this command. Default: Enabled. IS-IS performs consistency checks on hello packets and will form an adjacency only with a neighboring router that supports the same set of protocols.

Use the **no adjacency-check** command in address-family configuration mode to suppress the consistency checks for IPv6 IS-IS and allow an IPv4 IS-IS router to form an adjacency with a router running IPv4 IS-IS and IPv6. IS-IS will never form an adjacency between a router running IPv4 IS-IS only and a router running IPv6 only.

Send document comments to nexus7k-docfeedback@cisco.com

Use the **no adjacency-check** configuration mode command to suppress the IPv4 subnet consistency check and allow IS-IS to form an adjacency with other routers regardless of whether or not they have an IPv4 subnet in common. By default, IS-IS makes checks in hello packets for IPv4 address subnet matching with a neighbor.



Tip

Use the **debug isis adjacency packets** command in privileged EXEC mode to check for adjacency errors. Error messages in the output may indicate where routers are failing to establish adjacencies.

- **default-information originate [always] [route-map name]**—Controls the origination of a default route.
 - **always**—(Optional) Always advertises the default route.
 - **route-map name**—(Optional) Specifies the name of the route-map to announce the default routes.
- **distance value**—Specifies the administrative distance. To return to the default distance, use the **no** form of this command. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Range: 1 to 255. Default: 115.
- **distribute {level-1 | level-2} into {level-1 | level-2} {all | route-map name}**—Configures domain-wide prefix distribution between levels.
 - **level-1**—Distributes the interarea routes into level-1 of this IS-IS instance.
 - **level-2**—Distributes the interarea routes into level-2 of this IS-IS instance.
 - **into**—Specifies from one level to another level.
 - **all**—Distributes all route levels.
 - **route-map name**—Prevents distribution of a specific route-map.
- **exit**—Exits from the current command mode.
- **no**—Negates a command or set its defaults.
- **redistribute protocol as-num[.as-num] [route-map map-tag]**—Redistributes information from another routing protocol into IS-IS. To remove the **redistribute** command from the configuration file and return to the default setting, use the **no** form of this command. Default: Software does not redistribute routes. See the **redistribute (IS-IS)** command for information.
- **summary-address {ip-addr | ip-prefix/length | ipv6-addr | ipv6-prefix/length} level**—Creates the IS-IS aggregate addresses. To remove the aggregate address, use the **no** form of this command. See the **summary-address** command for information.

This command requires the Enterprise Services license.

Examples

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IPv4 address family:

```
switch(config)# router isis 100
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)#
```

The following example redistributes directly connected routes into IS-IS. This example advertises only 10.1.0.0 into the IS-IS level-1 link-state PDU.

```
switch(config)# router isis 100
switch(config-router)# address-family ipv4 unicast
```

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config-router-af)# redistribute direct route-map core1
switch(config-router-af)# summary-address 10.1.0.0 255.255.0.0
```

The following example shows how to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, enter the **no adjacency-check** command.

```
switch(config)# router isis test2
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# no adjacency-check
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

address-family (OSPFv3)

To enter address family mode for the Open Shortest Path First version 3(OSPFv3) protocol, use the **address-family** command.

address-family ipv6 unicast

Syntax Description	ipv6	Specifies the IPv6 address family.
	unicast	Specifies unicast address support.

Defaults This command has no default settings.

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command requires the Enterprise Services license.

Examples This example shows how to enter the IPv6 unicast address family for an OSPFv3v3 instance:

```
switch(config)# router ospfv3v3 Enterprise
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)#
```

Related Commands	Command	Description
	default-information (OSPFv3)	Controls the distribution of a default route.
	default-metric (OSPFv3)	Configures the default metric for routes redistributed into OSPFv3.
	distance (OSPFv3)	Configures the administrative distance.
	maximum-paths (OSPFv3)	Configures the maximum number of equal-cost paths.
	redistribute (OSPFv3)	Configures route redistribution for OSPFv3.
	timers (OSPFv3)	Configures the OSPFv3 timers.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults

This command has no default settings.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following 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.
timers	Configures the RIP timers.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

advertise-map

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* }

Syntax Description	<i>adv-map</i>	Route map with match statements that the route must pass before BGP passes the route to the next route map. The <i>adv-map</i> is a case-sensitive alphanumeric string up to 63 characters.
	exist-map <i>exist-rmap</i>	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 <i>exist-rmap</i> is a case-sensitive alphanumeric string up to 63 characters.
	non-exist-map <i>nonexist-rmap</i>	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 <i>nonexist-rmap</i> is a case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	BGP neighbor address-family command mode

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.2(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 <i>adv-map</i> and an <i>exist-map</i> or <i>nonexist-map</i> . The <i>exist-map</i> or <i>nonexist-map</i> specifies the prefix that the BGP tracks. The <i>adv-map</i> specifies the prefix that BGP advertises to the specified neighbor when the condition is met.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to configure BGP conditional advertisement:

```
switch# config t
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
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
```

Related Commands

Command	Description
feature bgp	Enables BGP.

Send document comments to nexus7k-docfeedback@cisco.com

advertisement-interval (VRRP)

To specify the time interval between the advertisement packets that are being sent to other 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

Syntax Description	<i>seconds</i>	Number of seconds between advertisement frames being sent. For IPv4, the range is from 1 to 255 seconds.

Defaults	1 second

Command Modes	VRRP configuration

Supported User Roles	network-admin VDC administrator

Command History	Release	Modified
	4.0(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.

This command does not require a license.

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)# vrrp 250
switch(config-if-vrrp)# advertisement-interval 200
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.
clear vrrp	Clears all the software counters for the specified virtual router.

Send document comments to nexus7k-docfeedback@cisco.com

aggregate-address

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	
<i>address/length</i>	Aggregate IP address and mask length. Valid values for <i>length</i> are as follows: - IPv4 addresses—1 to 32 - IPv6 addresses—1 to 128
advertise-map <i>map-name</i>	(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 <i>map-name</i>	(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 <i>map-name</i>	(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.

Defaults

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
Neighbor address-family configuration
Router BGP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

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

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP 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.)

Using 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.

Using 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 or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using 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.

Using 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.

Using 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 Enterprise Services license.

Examples

AS-Set Example

In the following example, an aggregate BGP address is created 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

In the following example, an aggregate BGP address is created in address family configuration mode and applied 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
```

Send document comments to nexus7k-docfeedback@cisco.com

```
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

In the following example, a route map called MAP-ONE is created 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)# !
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 <i>map-name</i>	Creates a route map.

Send document comments to nexus7k-docfeedback@cisco.com

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

<i>area-id</i>	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 <i>area-id</i> argument.

Defaults

No authentication

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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)# ip ospf area 0
switch(config-if)# ip ospf message-digest-key 10 md5 0 adcdefgh
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>area-id</i>	Identifier for the OSPF area where you want to configure the default cost. Specify as either a positive integer value or an IP address.
<i>cost</i>	Cost for the default summary route used for a stub or NSSA. The range is from 0 to 16777215.

Defaults

The summary route cost is based on the area border router that generated the summary route.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following example shows how to 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
```

Related Commands

Command	Description
area stub	Defines an area as a stub area.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area default-cost (OSPFv3)

To specify a cost for the default summary route sent into an Open Shortest Path First version 3(OSPFv3) 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

<i>area-id</i>	Identifier for the OSPFv3 area where you want to configure the default cost. Specify as either an IP address or a number from 0 to 4294967295.
<i>cost</i>	Cost for the default summary route used for a stub or NSSA. The range is from 0 to 16777215.

Defaults

The summary route cost is based on the area border router that generated the summary route.

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

This example shows how to a default cost of 20 to stub network 33:

```
switch(config)# router ospfv3 201
switch(config-router)# area 33 stub
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 33 default-cost 20
```

Related Commands

Command	Description
area stub	Defines an area as a stub area.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>area-id</i>	Identifier for the OSPF area where you want to configure filtering. Specify as either a positive integer value or an IP address.
route-map <i>map-name</i>	Specifies the name of a route map used as the filter policy. The <i>map-name</i> 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.

Defaults

None

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 NX-OS implicitly denies any prefix that does not match an entry in the route map.

This command requires the Enterprise Services license.

Examples

The following 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
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	area range	Consolidates and summarizes routes at an area boundary.
	route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area filter-list (OSPFv3)

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First version 3 (OSPFv3) 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

<i>area-id</i>	Identifier for the OSPFv3 area where you want to configure filtering. Specify as either an IP address or a number from 0 to 4294967295.
route-map <i>map-name</i>	Specifies the name of a route map used as the filter policy. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.
in	Filters networks sent to this area.
out	Filters networks sent from this area.

Defaults

None

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 NX-OS implicitly denies any prefix that does not match an entry in the route map.

This command requires the Enterprise Services license.

Examples

This example shows how to filter prefixes that are sent from all other areas to area 1:

```
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 1 filter-list route-map FilterExternal in
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	area range (OSPFv3)	Consolidates and summarizes routes at an area boundary.
	route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area nssa (OSPF)

To configure an area as an Open Shortest Path First (OSPF) not-so-stubby area (NSSA), 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. Specify as either a positive integer value or an IP address.
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on NSSA ABR or NSSA ASBR.
route-map <i>map-name</i>	(Optional) Filters the Type 7 default generation based on the route map. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.
no-redistribution	(Optional) Blocks redistributed LSAs from entering this NSSA area. Use this keyword when the router is both an NSSA autonomous system border router (ASBR) and an NSSA area border router (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.

Defaults

None

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

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 Enterprise Services license.

Examples

The following example shows how to configure area 1 as an NSSA area:

```
switch(config)# router ospf 10  
switch(config-router)# area 1 nssa
```

The following 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
```

Related Commands

Command	Description
redistribute	Redistributes routes learned from one routing protocol to another routing protocol domain.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area nssa (OSPFv3)

To configure an area as an Open Shortest Path First version 3 (OSPFv3) not-so-stubby area (NSSA), 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 OSPFv3 NSSA area. Specify as either an IP address or a number from 0 to 4294967295.
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on NSSA ABR or NSSA ASBR.
route-map <i>map-name</i>	(Optional) Filters the Type 7 default generation based on the route map. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.
no-redistribution	(Optional) Blocks redistributed LSAs from entering this NSSA area. Use this keyword when the router is both an NSSA autonomous system border router (ASBR) and an NSSA area border router (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.

Defaults

None

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Use the **area nssa** command to create an NSSA area in an OSPFv3 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 Enterprise Services license.

Examples

This example shows how to configure area 1 as an NSSA area:

```
switch(config)# router ospfv3 10  
switch(config-router)# area 1 nssa
```

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. (OSPFv3 places 0.0.0.0 as the forwarding address in the Type 5 LSAs.):

```
switch(config)# router ospfv3 2  
switch(config-router)# area 1 nssa translate type7 suppress-fa
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes routes learned from one routing protocol to another routing protocol domain.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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		
	<i>area-id</i>	Identifier for the OSPF area where you want to summarize routes. Specify as either a positive integer value or an IP address.
	<i>ip-prefix</i>	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.

Defaults Disabled

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples The following 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-router)# area 0 range 192.0.2.0 255.255.0.0
```


[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

area range (OSPFv3)

To consolidate and summarize routes at an Open Shortest Path First version 3 (OSPFv3) area boundary, use the **area range** command. To disable this function, use the **no** form of this command.

area *area-id* **range** *ipv6-prefix/length* [**not-advertise**]

no area *area-id* **range** *ipv6-prefix* [**not-advertise**]

Syntax Description	<i>area-id</i>	Identifier for the OSPF area where you want to summarize routes. Specify as either an IP address or a number from 0 to 4294967295.
	<i>ipv6-prefix/length</i>	IP prefix specified as IPv6 address/length (A:B::C:D/LEN). The <i>length</i> argument can be from 1 to 127.
	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.

Defaults	Disabled

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 OSPFv3 to summarize addresses for many different sets of address ranges by configuring multiple **area range** commands.

This command requires the Enterprise 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 2001:0DB8::/32:

```
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# area 0 range 2001:0DB8::/32
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>area-id</i>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.
	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Defaults	None

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 LSAs) into the stub area.

This command requires the Enterprise Services license.

Examples	The following example shows how to create stub area 33 in OSPF 209:

```
switch(config)# router ospf 201
switch(config-router)# area 33 stub
```

Related Commands	Command	Description
	area default-cost	Specifies a cost for the default summary route sent into a stub area.

Send document comments to nexus7k-docfeedback@cisco.com

area stub (OSPFv3)

To define an area as an Open Shortest Path First version 3 (OSPFv3) 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	<i>area-id</i>	Identifier for the OSPFv3 stub area. Specify as either an IP address or a number from 0 to 4294967295.
	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Defaults	None

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 LSAs) into the stub area.

This command requires the Enterprise Services license.

Examples	This example shows how to create stub area 33 in OSPFv3 209:

```
switch(config)# router ospfv3 201  
switch(config-router)# area 33 stub
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
area default-cost (OSPFv3)	Specifies a cost for the default summary route sent into a stub area.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>area-id</i>	Identifier for the OSPF area assigned to the transit area for the virtual link. Specify as either a positive integer value or an IP address.
	<i>router-id</i>	Router ID associated with the virtual link neighbor. Specify as an IP address. The router ID appears in the show ip ospf neighbors display.

Defaults	None

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

This command requires the Enterprise Services license.

Examples

The following 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
```

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
```

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.
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.
transmit-delay (OSPF virtual link)	Configures the transmit delay for an OSPF virtual link.

Send document comments to nexus7k-docfeedback@cisco.com

area virtual-link (OSPFv3)

To define an Open Shortest Path First version 3 (OSPFv3) 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	<i>area-id</i>	Identifier for the OSPFv3 area assigned to the transit area for the virtual link. Specify as either an IP address or a number from 0 to 4294967295.
	<i>router-id</i>	Router ID associated with the virtual link neighbor. Specify as an IP address. The router ID appears in the show ospfv3 neighbors display.

Defaults	None

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 OSPFv3, 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:

- **dead-interval** *seconds*
- **hello-interval** *seconds*
- **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 ospfv3 neighbors** command in any mode.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

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 ospfv3 1
switch(config-router)# router-id 192.0.2.2
switch(config-router)# area 1 virtual-link 192.0.2.1
```

Device B:

```
switch(config)# router ospfv3 209
switch(config-router)# router-id 192.0.2.1
switch(config-router)# area 1 virtual-link 192.0.2.2
```

Related Commands

Command	Description
dead-interval (OSPFv3 virtual link)	Configures the dead interval for an OSPFv3 virtual link.
hello-interval (OSPFv3 virtual link)	Configures the hello interval for an OSPFv3 virtual link.
retransmit-interval (OSPFv3 virtual link)	Configures the retransmit interval for an OSPFv3 virtual link.
transmit-delay (OSPFv3 virtual link)	Configures the transmit delay for an OSPFv3 virtual link.

Send document comments to nexus7k-docfeedback@cisco.com

authentication (GLBP)

To configure an authentication for the Gateway Load Balancing Protocol (GLBP), use the **authentication** command. To disable authentication, use the **no** form of this command.

authentication {**text** *string* | **md5** {**key-string** [**encrypted**] *key* | **key-chain** *name-of-chain*}}

no authentication {**text** *string* | **md5** {**key-string** [**0** | **7**] *key* | **key-chain** *name-of-chain*}}

Syntax Description

text <i>string</i>	Specifies an authentication string. The range is from 1 to 255 characters.
md5	Specifies the Message Digest 5 (MD5) authentication.
key-string <i>key</i>	Specifies the secret key for MD5 authentication. The range is from 1 to 255 characters. We recommend that you use at least 16 characters.
encrypted	(Optional) Specifies the encrypted key.
key-chain <i>name-of-chain</i>	Identifies a group of authentication keys.

Defaults

No authentication of GLBP messages occurs.

Command Modes

GLBP configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To ensure interoperation, you must configure the same authentication method on all the gateways that are members of the same GLBP group. A gateway ignores all GLBP messages that contain the wrong authentication information.

This command does not require a license.

Examples

The following example shows how to configure stringxyz as the authentication string for GLBP group 10:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# authentication text stringxyz
```

The following example shows how to configure GLBP to use the key chain "AuthenticateGLBP" to obtain the current live key and key ID for MD5 authentication:

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# interface ethernet1/1
switch(config-if)# glbp 2
switch(config-glbp)# authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp	Creates a GLBP group and enters GLBP configuration mode.
ip (GLBP)	Enables GLBP on an interface.
key chain	Creates a key chain.

Send document comments to nexus7k-docfeedback@cisco.com

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 {text string | md5 {key-chain key-chain | key-string {0 | 7} text [timeout
seconds]}}
```

```
no authentication {text string | md5 {key-chain key-chain | key-string {0 | 7} text [timeout
seconds]}}
```

Syntax Description		
text <i>string</i>		Specifies an authentication string. The range is from 1 to 255 characters. The default string is "cisco".
md5		Specifies the Message Digest 5 (MD5) authentication.
key-chain <i>key-chain</i>		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.
<i>text</i>		The secret key for MD5 authentication. The range is from 1 to 255 characters. We recommend that you use at least 16 characters.
timeout <i>seconds</i>		(Optional) Specifies the authentication timeout value. The range is from 0 to 32767.

Defaults Disabled

Command Modes HSRP configuration or HSRP template mode

SupportedUserRoles network-admin
VDC administrator

Command History	Release	Modification
	4.0(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 two routers are configured with identical HSRP IP addresses, but with different authentication strings, then neither router will be aware of the duplication.

Send document comments to nexus7k-docfeedback@cisco.com

This command does not require a license.

Examples

The following example shows how to configure an authentication string for HSRP group 2:

```
switch# configure terminal
switch(config)# interface ethernet 0/1
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
```

Related Commands

Command	Description
feature hsrp	Enable HSRP and enters HSRP configuration mode.
hsrp group	Creates an HSRP group.

Send document comments to nexus7k-docfeedback@cisco.com

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 ip ospf authentication

Syntax Description

key-chain <i>key-name</i>	(Optional) Specifies the key-chain to use. The <i>key-name</i> 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.

Defaults

Defaults to password authentication if you configure authentication with none of the optional keywords.

Command Modes

OSPF virtual link configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

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

Syntax Description	text <i>password</i> Selects to use simple text password of up to 8 alphanumeric characters.	
Defaults	No authentication	
Command Modes	VRRP configuration mode	
Supported User Roles	network-admin VDC administrator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure md5 authentication for VRRP: switch# config t switch(config)# interface ethernet 2/1 switch(config-if)# vrrp 250 switch(config-if-vrrp)# authentication text mypassword	
Related Commands	Command	Description
	show vrrp	Displays VRRP configuration information.
	clear vrrp	Clears all the software counters for the specified virtual router.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>name-of-chain</i>	Group of keys that are valid.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Router configuration
Address family configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(3)	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 Enterprise Services license.

Examples

The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

authentication key-chain (IS-IS)

To enable authentication for Intermediate System-to-Intermediate System (IS-IS), use the **authentication key-chain** configuration mode command. To disable such authentication, use the **no** form of this command.

authentication key-chain *auth-key* {**level-1** | **level-2**}

no authentication key-chain *auth-key* {**level-1** | **level-2**}

Syntax Description

<i>auth-key</i>	Authentication key chain.
level-1	Specifies the authentication key for level-1 link state packets (LSP), complete sequence number packets (CSNP), and partial sequence number packets (PSNP) only.
level-2	Specifies the authentication key for level-2 LSP, CSNP and PSNP packets only.

Command Default

No key chain authentication is provided for IS-IS packets at the router level.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If no key chain is configured with the **authentication key-chain** command, no key chain authentication is performed.

Key chain authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the authentication mode command.

Only one authentication key chain is applied to IS-IS at one time. For example, if you configure a second **authentication key-chain** command, the first authentication key chain is overridden.

You can specify authentication for an individual IS-IS interface by using the **isis authentication key-chain** command.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example configures IS-IS to accept and send any key belonging to the key chain named site1:

```
switch(config)# router isis real_secure_network  
switch(config-router)# authentication key-chain site1 level-1
```

Related Commands

Command	Description
exit	Exits the current configuration mode.
feature isis	Enables IS-IS on the router.
isis authentication key-chain	Enables authentication for an individual IS-IS interface.
no	Negates a command or sets its defaults.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults

None

Command Modes

Router configuration
Address family configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following 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
```

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.

Send document comments to nexus7k-docfeedback@cisco.com

authentication-check

To specify for the Intermediate System-to-Intermediate System (IS-IS) instance that authentication is performed only on IS-IS packets being sent (not received), use the **authentication-check** configuration mode command. To configure for the IS-IS instance that if authentication is configured at the router level, such authentication be performed on packets being sent and received, use the **no** form of this command.

authentication-check {level-1 | level-2}

no authentication-check

Syntax Description	level-1	Specifies that authentication is performed only on level-1 packets that are being sent (not received)
	level-2	Specifies that authentication is performed only on level-2 packets that are being sent (not received).

Command Default	If authentication is configured at the router level, it applies to IS-IS packets being sent and received.

Command Modes	Router configuration VRF configuration

Usage Guidelines	Enter the authentication-check command before configuring the authentication mode and authentication key chain. Entering the authentication-check command allows the routers to have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After you enter the authentication-check command on all communicating routers, enable the authentication mode and key chain on each router. Then enter the no authentication-check command to disable the command.

This command could apply to clear text authentication or Message Digest 5 (MD5) authentication. The mode is determined by the authentication mode command.

You can specify authentication for an individual IS-IS interface by using the **isis authentication-check {level-1 | level-2}** interface configuration mode command.

This command requires the Enterprise Services license.

Examples	The following example configures IS-IS level-1 packets to use clear text authentication on packets being sent (not received):

```
switch(config)# router isis test1
switch(config-router)# authentication-check level-1
switch(config-router)# authentication key-chain site1 level-1
switch(config-router)#
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
isis authentication-check	Enables authentication on IS-IS packets being sent (not received) from a specific interface.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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.
	<i>password</i>	Any continuous string of characters that can be entered from the keyboard up to 8 bytes.

Defaults	Unencrypted password

Command Modes	OSPF virtual link configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

authentication-type

To specify the type of authentication used in Intermediate System-to-Intermediate System (IS-IS) packets for the IS-IS instance, use the **authentication-type** configuration mode command. To restore clear text authentication, use the **no** form of this command.

authentication-type { cleartext | md5 } [level-1 | level-2]

no authentication-type

Syntax Description

cleartext	Specifies clear text authentication.
md5	Specifies Message Digest 5 (MD5) authentication.
level-1	Enables the specified authentication for level-1 link state packet (LSP), complete sequence number packet (CSNP) and partial sequence number packet (PSNP) packets only.
level-2	Enables the specified authentication for level-2 LSP, CSNP and PSNP packets only.

Command Default

No authentication is provided for IS-IS packets at the router level by use of this command.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If you do not enter the **level-1** or **level-2** keywords, the mode applies to both levels.

You can specify the type of authentication and the level to which it applies for a single IS-IS interface, rather than per IS-IS instance, by using the **authentication-type** command.

You can specify authentication type for an individual IS-IS interface by using the **isis authentication-type { cleartext | md5 } [level-1 | level-2]** interface configuration mode command.

Examples

The following example configures for the IS-IS instance that Message Digest 5 (MD5) authentication is performed on level-1 packets:

```
switch(config)# router isis TEST1
switch(config-router)# authentication-type md5 level-1
switch(config-router)#
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	exit	Exits the current configuration mode.
	feature isis	Enables IS-IS on the router.
	isis authentication-type	Specifies the authentication type for an individual IS-IS interface.
	no	Negates a command or sets its defaults.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 40Gb/s, use the **no** form of this command.

auto-cost reference-bandwidth *bandwidth* [Gbps | Mbps]

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth <i>bandwidth</i>	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.

Defaults

40 Gb/s. The bandwidth defaults to Gb/s if you do not specify the **Gbps** or **Mbps** keyword.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
ip ospf cost	Explicitly specifies the cost of sending a packet on an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

auto-cost (OSPFv3)

To control how Open Shortest Path First version 3 (OSPFv3) calculates default metrics for an interface, use the **auto-cost** command. To assign the default reference bandwidth of 40Gb/s, use the **no** form of this command.

auto-cost reference-bandwidth *bandwidth* [Gbps | Mbps]

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth <i>bandwidth</i>	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.

Defaults

40 Gb/s. The bandwidth defaults to Gb/s if you do not specify the **Gbps** or **Mbps** keyword.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **auto-cost** command to set the reference bandwidth used by the OSPFv3 cost-metric calculation. The value set by the **ipv6 ospfv3 cost** command overrides the cost that results from the **auto-cost** command.

This command requires the Enterprise Services license.

Examples

This example shows how to set the reference bandwidth for all local interfaces in an OSPFv3 instance:

```
switch(config)# router ospfv3 201
switch(config-router)# auto-cost reference-bandwidth 10
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	ipv6 ospfv3 cost	Explicitly specifies the cost of sending a packet on an interface.

Send document comments to nexus7k-docfeedback@cisco.com

autonomous-system

To configure the autonomous system 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

<i>as-number</i>	Autonomous system number. The range is from 1 to 65535.

Defaults

None

Command Modes

Address family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	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 Enterprise Services license.

Examples

The following example shows how to set an AS number for EIGRP for IPv6 unicast:

```
switch(config)# router eigrp 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# autonomous-system 64496
```

Related Commands

Command	Description
address-family (EIGRP)	Enters the address family configuration mode for EIGRP.



B Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter B.

bestpath

To change the default bestpath selection algorithm, use the **bestpath** router bgp configuration mode command. To return the 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 different 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. Default: A value of 0 is assigned to the missing MED.
med non-deterministic	Specifies that the best-MED path among paths is not picked from the same AS. Default: Disabled.

Command Default

This command has no default settings.

Command Modes

Router BGP configuration
Neighbor configuration
VRF configuration

Send document comments to nexus7k-docfeedback@cisco.com

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

You must ensure that BGP is enabled prior to entering this command for this command to be supported. You can enter the **feature bgp** global configuration mode command to enable BGP.

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 Enterprise Services license.

Examples

The following example shows how to change the default bestpath selection algorithm to compare the MED on paths from different AS:

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

Related Commands	Command	Description
	feature bgp	Enables BGP globally.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com



C Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter C.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear bgp

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

```
clear bgp [{ipv4 | ipv6} {unicast | multicast} | all] {neighbor | * | as-number | peer-template
name | prefix} [vrf vrf-name]
```

Syntax Description

ipv4	(Optional) Clear BGP information for IPv4 address family.
ipv6	(Optional) Clear BGP information for IPv6 address family.
unicast	Clears BGP information for unicast address family.
multicast	Clears BGP information for multicast address family.
all	(Optional) Clear BGP information for all address families.
<i>neighbor</i>	A network address. The format is A.B.C.D for IPv4 and A:B::C:D for IPv6.
<i>as-number</i>	Autonomous system number. The range is from 1 to 65535.
vrf <i>vrf-name</i>	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.
peer-template <i>name</i>	Specifies a BGP peer template. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>prefix</i>	A prefix from the selected address family. The format is A.B.C.D/length for IPv4 and A:B::C:D/length for IPv6.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Added support for IPv6 prefixes.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear all BGP entries:

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear bgp dampening

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

```
clear bgp { {ipv4 | ipv6} {unicast | multicast} | all} dampening [neighbor | prefix] [vrf vrf-name]
```

Syntax Description	ipv4	(Optional) Clears BGP information for IPv4 address family.
	ipv6	(Optional) Clears BGP information for IPv6 address family.
	unicast	Clears BGP information for unicast address family.
	multicast	Clears BGP information for multicast address family.
	all	(Optional) Clears BGP information for all address families.
	<i>neighbor</i>	A neighbor from the selected address family. The format is A.B.C.D for IPv4.
	<i>prefix</i>	A 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 instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear BGP route flap dampening information: switch# clear bgp all dampening

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear bgp flap-statistics

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

clear bgp flap-statistics [*neighbor* | *prefix*] [**vrf** *vrf-name*]

Syntax Description		
	<i>neighbor</i>	A neighbor from the selected address family. The format is A.B.C.D for IPv4.
	<i>prefix</i>	A prefix from the selected address family. The format is A.B.C.D/length for IPv4.
	vrf <i>vrf-name</i>	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear BGP route flap statistics: switch# clear bgp flap-statistics

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>prefix</i>	Summary address. Format is x.x.x.x or x.x.x.x/length. The length range is from 1 to 32.
	advertise-map	Clears policy statistics for the advertise policy
	suppress-map	Clears policy statistics for the suppress policy.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Examples	The following 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 policy statistics for bgp.

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear policy statistics for dampening:

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

Related Commands

Command	Description
show bgp policy statistics	Displays policy statistics for bgp.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>prefix</i>	Neighbor address. Format is x.x.x.x.
	default-originate	Clears policy statistics for the default originate policy.
	filter-list	Clears policy statistics for the neighbor filter list.
	prefix-list	Clears policy statistics for the neighbor prefix list.
	route-map	Clears policy statistics for the neighbor route map.
	in	Clears inbound policy statistics.
	out	Clears outbound policy statistics.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear policy statistics for an aggregate address: <pre>switch# clear bgp policy statistics neighbor 192.0.2.1 filter-list in</pre>

Related Commands	Command	Description
	show bgp policy statistics	Displays policy statistics for BGP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear bgp policy statistics redistribute

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

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

Syntax Description

vrf <i>vrf-name</i> *	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.
direct	Clears policy statistics for directly connected routes only.
eigrp	Clears policy statistics for EIGRP.
isis	Clears policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
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.
<i>id</i>	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 NX-OS stores it internally as a string. For the isis keyword, an IS-IS 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 NX-OS 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 NX-OS stores it internally as a string.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to clear policy statistics for RIP:

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

Related Commands

Command	Description
show bgp policy statistics	Displays policy statistics for bgp.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear forwarding route

To clear forwarding information, use the **clear forwarding route** command.

clear forwarding {**ip** | **ipv4** | **ipv6**} **route** [***** | *prefix*] [**vrf** *vrf-name*]

Syntax Description		
ip		Clears an IPv4 route.
ipv4		Clears an IPv4 route.
ipv6		Clears an IPv6 route.
*		Clears all routes.
<i>prefix</i>		An IPv4 or IPv6 prefix. The IPv4 format is x.x.x.x/length. The IPv6 format is A:B::C:D/length.
vrf <i>vrf-name</i>		(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example clears a route from the FIB: switch# clear forwarding ip 10.0.0.1/8

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 [ip | ipv4 | ipv6] [unicast] [vrf vrf-name] [module {slot| all}]
```

Syntax Description

ip	(Optional) Specifies the inconsistency check for IPv4 routes.
ipv4	(Optional) Specifies the inconsistency check for IPv4 routes.
ipv6	(Optional) Specifies the inconsistency check for IPv6 routes.
unicast	(Optional) Specifies the inconsistency check for unicast routes.
module	(Optional) Specifies the inconsistency check for one or more modules.
<i>slot</i>	Module number. The range depends on the platform.
all	(Optional) Specifies the inconsistency check for all modules.

Defaults

None

Command Modes

Any

Supported User Roles

Network Administrator
VDC Administrator

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added support for ipv6 keyword.

Usage Guidelines

This command does not require a license.

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear hardware ip verify

To clear IP packet verification, use the **clear hardware ip verify** command. To disable IP packet verification, use the **no** form of this command.

clear hardware ip verify {checksum | fragment | protocol | tcp tiny-frag | version}

Syntax Description	checksum	Drops IPv4 or IPv6 packets if the checksum is invalid
	fragment	Drops IPv4 or IPv6 packets if the packet fragment has a nonzero offset and the DF bit is active.
	protocol	Drops IPv4 or IPv6 packets if the packet fragment has an invalid IP protocol number.
	tcp tiny-frag	Drops IPv4 packets if the IP fragment offset is 1, or if the IP fragment offset is 0 and the IP payload length is less than 16.
	version	Drops IPv4 packets if the ethertype is not set to 4 (IPv4).

Defaults None.

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.1(3)	This command was introduced.
	4.2(2)	Added protocol keyword.

Usage Guidelines Use the **clear hardware ip verify** command to clear packet verification tests on IPv4 and IPv6 packets based on checksum or fragments.

This command does not require a license.

Examples This example shows how to clear fragmented IPv4 or IPv6 packet tests:

```
switch(config)# clear hardware ip verify fragment
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
	hardware ip verify length	Configures IPv4 packet verification checks based on length.
	hardware ipv6 verify	Configures IPv6 packet verification.
	show hardware forwarding ip verify	Displays information about IP packet verification checks.

Send document comments to nexus7k-docfeedback@cisco.com

clear hardware ip verify address

To clear packet verification tests on IP addresses, use the **clear hardware ip verify address** command. To disable packet verification tests, use the **no** form of this command.

clear hardware ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}

Syntax Description		
	destination zero	Drops IP packets if the destination IPv4 address is 0.0.0.0 or if the IPv6 address is ::.
	identical	Drops IP packets if the source IPv4 or IPv6 address is identical to the destination IPv4 or IPv6 address.
	reserved	Drops IP packets if the IPv4 address is in the 127.x.x.x range or if the IPv6 address is in the ::1 range.
	source	Drops IP packets based on the IP source address
	broadcast	Drops IP packets if the IP source address is 255.255.255.255
	multicast	Drops IP packets if the IPv4 source address is in the 224.x.x.x range or if the IPv6 source address is in the FF00::/8 range.

Defaults	None

Command Modes	Global configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines

Use the **clear hardware ip verify address** command to clear packet verification tests on IPv4 and IPv6 packets based on addresses.

This command does not require a license.

Examples

This example shows how to clear broadcast IPv4 packet tests:

```
switch(config)# clear hardware ip verify address source broadcast
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	hardware ip verify	Configures IPv4 and IPv6 packet verification checks based on checksum or fragments.
	hardware ip verify length	Configures IPv4 packet verification checks based on length.
	hardware ipv6 verify	Configures IPv6 packet verification.
	show hardware forwarding ip verify	Displays information about IP packet verification checks.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear hardware ip verify length

To clear IPv4 packet verification tests based on packet length, use the **clear hardware ip verify length** command. To disable the tests, use the **no** form of this command.

clear hardware ip verify length { consistent | maximum { max-frag | max-tcp | udp } | minimum }

Syntax Description	consistent	Drops IPv4 packets where the Ethernet frame size is greater than or equal to the IP packet length plus the Ethernet header.
	maximum { max-frag max-tcp udp }	Drops IPv4 packets based on the following: • max-frag—Drops IP packets if the maximum fragment offset is greater than 65536. • max-tcp—Drops IP packets if the TCP length is greater than the IP payload length. • udp—Drops IP packets if the IP payload length is less than the UDP packet length.
	minimum	Drops IP packets if the Ethernet frame length is less than the IP packet length plus four octets (the CRC length).

Defaults	None

Command Modes	Global configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines	Use the clear hardware ip verify length command to clear packet verification tests on IPv4 and IPv6 packets based on packet length.

This command does not require a license.

Examples	This example shows how to clear minimum-length IPv4 packet tests:
	switch(config)# clear hardware ip verify length minimum

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
hardware ip verify	Configures IPv4 packet verification checks based on checksum or fragments.
hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
hardware ipv6 verify	Configures IPv6 packet verification.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example clears the adjacency statistics: switch# clear ip adjacency statistics

Related Commands	Command	Description
	show ip adjacency	Displays adjacency information.

Send document comments to nexus7k-docfeedback@cisco.com

clear ip arp

To clear the Address Resolution Protocol (ARP) information, use the **clear ip arp** command.

clear ip arp [*ip-addr* | *interface*] [**statistics**] [**vrf** *vrf-name*]

Syntax Description	<i>ip-addr</i>	(Optional) An IPv4 source address. The format is x.x.x.x.
	<i>interface</i>	(Optional) An interface. Use ? to determine the supported interface types.
	statistics	(Optional) Clears ARP statistics.
	<i>vrf vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	The following example clears the ARP table:	
	switch# clear ip arp	
Related Commands	Command	Description
	show ip arp	Displays information about ARP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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}] {neighbor | * | as-number | peer-template name | prefix}
               [vrf vrf-name]
```

Syntax Description		
ipv4	(Optional) Clear BGP information for IPv4 address family.	
unicast	Clears BGP information for unicast address family.	
multicast	Clears BGP information for multicast address family.	
all	(Optional) Clear BGP information for all address families.	
<i>neighbor</i>	A network address. The format is A.B.C.D for IPv4 and A:B::C:D for IPv6.	
<i>as-number</i>	Autonomous system number. The range is from 1 to 65535.	
vrf <i>vrf-name</i>	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.	
peer-template <i>name</i>	Specifies a BGP peer template. The name can be any case-sensitive alphanumeric string up to 63 characters.	
<i>prefix</i>	A prefix from the selected address family. The format is A.B.C.D/length for IPv4 and A:B::C:D/length for IPv6.	

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear all BGP entries for the IPv4 address family: <pre>switch# clear ip bgp *</pre>

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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}} dampening [neighbor | prefix] [vrf vrf-name]
```

Syntax Description	ipv4	(Optional) Clears BGP information for IPv4 address family.
	unicast	Clears BGP information for unicast address family.
	multicast	Clears BGP information for multicast address family.
	<i>neighbor</i>	A neighbor from the selected address family. The format is A.B.C.D for IPv4.
	<i>prefix</i>	A 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 instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear BGP route flap dampening information: switch# clear ip bgp dampening

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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*]

Syntax Description		
	<i>neighbor</i>	A neighbor from the selected address family. The format is A.B.C.D for IPv4.
	<i>prefix</i>	A prefix from the selected address family. The format is A.B.C.D/length for IPv4.
	vrf <i>vrf-name</i>	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear BGP route flap statistics: switch# clear ip bgp flap-statistics

Send document comments to nexus7k-docfeedback@cisco.com

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 [*instance-tag*] **accounting** [**vrf** {*vrf-name* | *}]

Syntax Description	<i>instance-tag</i>	(Optional) Instance tag. 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 63 characters.
	vrf <i>vrf-name</i>	(Optional) Name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
	vrf *	(Optional) Specifies all VRF instances.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear the EIGRP accounting information: switch# clear ip eigrp accounting

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 in EXEC mode.

```
clear ip eigrp [instance-tag] neighbors [* | ip-address | interface-type interface-instance] [soft]
[vrf {vrf-name | *}]
```

Syntax Description

<i>instance-tag</i>	(Optional) Instance identifier. The instance-tag can be any case-sensitive alphanumeric string up to 63 characters.
*	(Optional) Clears all neighbors.
<i>ip-address</i>	(Optional) Address of the neighbor.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) CLI help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance. Specifying these arguments removes the specified interface type from the neighbor table that all entries learned via this interface. For more information about the interface syntax, use the question mark (?) online help function.
soft	(Optional) Specifies soft reset for the neighbors.
vrf { <i>vrf-name</i> *}	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name is an alphanumeric string of up to 32 characters.

Defaults

When no autonomous system number, interface, or VRF instance is specified, all EIGRP neighbor entries are cleared from the table.

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Added * and soft keywords.

Usage Guidelines

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to clear all EIGRP entries for neighbors on Ethernet interface 2/1:

```
switch# clear ip eigrp vrf * neighbors ethernet 2/1
```

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip eigrp policy statistics redistribute

To clear policy statistics for routes redistributed into the the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **clear ip eigrp policy statistics redistribute** command.

```
clear ip eigrp policy statistics redistribute {bgp id | direct | eigrp id | isis id | ospf id | rip 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 EIGRP.
isis	Clears policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
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.
<i>id</i>	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 NX-OS stores it internally as a string. For the isis keyword, an IS-IS 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 NX-OS 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 NX-OS 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.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	This command was removed and replaced by the clear ip eigrp route-map statistics command.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear policy statistics for RIP:

```
switch# clear ip eigrp policy statistics redistribute rip 201
```

Related Commands

Command	Description
show ip eigrp policy statistics	Displays policy statistics for EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip eigrp policy statistics redistribute

To clear policy statistics for routes redistributed into the the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **clear ip eigrp policy statistics redistribute** command.

```
clear ip eigrp policy statistics redistribute {bgp id | direct | eigrp id | isis id | ospf id | rip 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 EIGRP.
isis	Clears policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
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.
<i>id</i>	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 NX-OS stores it internally as a string. For the isis keyword, an IS-IS 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 NX-OS 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i> *	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	This command was removed and replaced by the clear ip eigrp route-map statistics command.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear policy statistics for RIP:

```
switch# clear ip eigrp policy statistics redistribute rip 201
```

Related Commands

Command	Description
show ip eigrp policy statistics	Displays policy statistics for EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip eigrp redistribution

To clear redistribution information for Enhanced Interior Gateway Routing Protocol (EIGRP) , use the **clear ip eigrp redistribution** command.

clear ip eigrp redistribution [**vrf** {*vrf-name* | *}]

Syntax Description

vrf <i>vrf-name</i> *	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear redistribution information:

```
switch# clear ip eigrp redistribution
```

Related Commands

Command	Description
feature eigrp	Enables the EIGRP feature.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 [instance-tag] traffic [vrf {vrf-name | *}]
```

Syntax Description	<i>instance-tag</i>	(Optional) Instance of EIGRP. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
	vrf <i>vrf-name</i>	(Optional) Name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
	vrf *	(Optional) Specifies all VRF instances.

Defaults	This command clears information for the default VRF if no VRF is specified.

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear the EIGRP traffic statistics: switch# clear ip eigrp traffic

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example clears the IP interface statistics: switch# clear ip interface statistics

Related Commands	Command	Description
	show ip interface	Displays IP interface information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip mbgp

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

```
clear ip mbgp {neighbor | * | as-number | peer-template name | prefix} [vrf vrf-name]
```

Syntax Description	<i>neighbor</i>	A network address. The format is A.B.C.D for IPv4.
	<i>as-number</i>	Autonomous system number. The range is from 1 to 65535.
	vrf <i>vrf-name</i>	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.
	peer-template <i>name</i>	Specifies a BGP peer template. The name can be any case-sensitive alphanumeric string up to 63 characters.
	<i>prefix</i>	A prefix from the selected address family. The format is A.B.C.D/length for IPv4.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear all MBGP entries for the IPv4 address family: switch# clear ip mbgp *

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip mbgp dampening

To clear Multiprotocol Border Gateway Protocol (MBGP) route flap dampening information, use the **clear ip mbgp dampening** command.

clear ip mbgp dampening [**neighbor** | **prefix**] [**vrf** *vrf-name*]

Syntax Description		
	<i>neighbor</i>	A neighbor from the selected address family. The format is A.B.C.D for IPv4.
	<i>prefix</i>	A prefix from the selected address family. The format is A.B.C.D/length for IPv4.
	vrf <i>vrf-name</i>	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear MBGP route flap dampening information: switch# clear ip mbgp dampening

Send document comments to nexus7k-docfeedback@cisco.com

clear ip mbgp flap-statistics

To clear Multiprotocol Border Gateway Protocol (MBGP) route flap statistics, use the **clear ip mbgp flap-statistics** command.

clear ip mbgp flap-statistics [*neighbor* | *prefix*] [**vrf** *vrf-name*]

Syntax Description	<i>neighbor</i>	A neighbor from the selected address family. The format is A.B.C.D for IPv4.
	<i>prefix</i>	A prefix from the selected address family. The format is A.B.C.D/length for IPv4.
	vrf <i>vrf-name</i>	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear MBGP route flap statistics: switch# clear ip mbgp flap-statistics

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.
*	Clears all neighbors.
<i>neighbor-id</i>	Specifies the Neighbor ID (as an IP address) of the neighbor to clear.
<i>interface-type number</i>	Specifies interface from which to clear all neighbors.
loopback <i>number</i>	Clears all neighbors on a loopback interface.
port-channel <i>number</i>	Clears all neighbors on a port-channel interface.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPF virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 NX-OS clears the neighbor details from all OSPF instances. Use the **show ip ospf neighbor** command to find the neighbor ID.

This command requires the Enterprise Services license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

The following example shows how to clear all OSPF neighbor details for all OSPF instances:

```
switch# clear ip ospf neighbor *
```

The following example shows how to clear all OSPF neighbor details for all neighbors on Ethernet interface 1/2 for OSPF instance 202:

```
switch# clear ip ospf 202 neighbor ethernet 1/2
```

Related Commands

Command	Description
<code>show ip ospf neighbor</code>	Displays details for OSPF neighbors including the neighbor ID.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 | isis id | ospf id | rip id | static}} [vrf vrf-name]
```

Syntax	Description
<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.
area	Clears policy statistics for an area.
<i>area-id</i>	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 <i>autonomous-system</i>	Specifies the autonomous system number for the Border Gateway Protocol. Specify the autonomous system number as <i>x.y</i> , where the range is from 1 to 65535 for both <i>x</i> and <i>y</i> , or as a single integer, where the range is from 1 to 65535.
direct	Specifies directly connected routes.
eigrp <i>id</i>	Specifies the autonomous system number for the Enhanced Interior Gateway Protocol. Specify the <i>id</i> argument as any case-sensitive alphanumeric string.
isis <i>id</i>	Specifies the Intermediate System to Intermediate System instance. Specify the <i>id</i> argument as any case-sensitive alphanumeric string.
ospf <i>id</i>	Specifies the Open Shortest Path First version 2 instance. Specify the <i>id</i> argument as any case-sensitive alphanumeric string.
rip <i>id</i>	Specifies the Routing Information Protocol instance. Specify the <i>id</i> argument as any case-sensitive alphanumeric string.
static	Specifies static routes.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPF virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.

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 NX-OS clears the policy statistics from all OSPF instances. Use the **show ip ospf policy statistics** command to view the statistics that you are clearing.

This command requires the Enterprise Services license.

Examples

The following 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
```

The following 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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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* | *}]

Syntax Description

vrf <i>vrf-name</i> *	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear redistribution information:

```
switch# clear ip ospf redistribution
```

Related Commands

Command	Description
feature ospf	Enables the OSPF feature.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPF virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 <i>instance-tag</i> argument, Cisco NX-OS clears statistics from all OSPF instances. Use the show ip ospf statistics command to view the statistics that you are clearing. This command requires the Enterprise Services license.	
Examples	The following example shows how to clear all OSPF event statistics: <pre>switch# clear ip ospf statistics</pre>	
Related Commands	Command	Description
	show ip ospf statistics	Displays event statistics for OSPF.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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		
<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 20 characters.	
<i>interface</i>	(Optional) Interface to clear traffic statistics for. Use the ? option to see the interface options.	
vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPF virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string of up to 32 characters, except “default” and “all”.	

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	Added <i>interface</i> argument.

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 <i>instance-tag</i> argument, Cisco NX-OS 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 Enterprise Services license.

Examples	The following example shows how to clear OSPF traffic statistics for OSPF 100: <pre>switch# clear ip ospf 100 traffic</pre>

Related Commands	Command	Description
	show ip ospf traffic statistics	Displays OSPF traffic statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip rip policy statistics redistribute

To clear policy statistics for routes redistributed into the 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 | isis id | ospf id | ospfv3 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).
isis	Clears policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
ospf	Clears policy statistics for the Open Shortest Path First (OSPF) protocol.
ospfv3	Clears policy statistics for the Open Shortest Path First version 3 (OSPFv3) protocol.
static	Clears policy statistics for IP static routes.
<i>id</i>	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 NX-OS stores it internally as a string. For the isis keyword, an IS-IS 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 NX-OS stores it d 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 NX-OS stores it internally as a string.
vrf vrf-name	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. Length is up to 32 alphanumeric characters.

Defaults This command has no default settings.

Command Modes Any

Supported User Roles network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

clear ip rip statistics

To clear the 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 <i>type instance</i>	(Optional) Specifies the interface to clear topology entries.
vrf [<i>vrf-name</i>]	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is up to 32 alphanumeric characters.

Defaults

This command has no default settings.

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following 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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip route

To clear individual routes from the unicast RIB, use the **clear ip route** command.

clear ip route [* | *addr* | *prefix*]] [**vrf** *vrf-name*]

Syntax Description	
*	(Optional) Clears all routes.
<i>addr</i>	(Optional) Clears this route. The format is x.x.x.x.
<i>addr</i>	(Optional) Clears this prefix. The format is x.x.x.x/length.
vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines	Use the clear ip route command to clear individual routes from the route table.



Note

The * keyword is severely disruptive to routing.

This command does not require a license.

Examples	The following example clears 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.

Send document comments to nexus7k-docfeedback@cisco.com

clear ip traffic

To clear IP traffic information, use the **clear ip traffic** command.

clear ip traffic

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example clears the IP traffic information: switch(config)# clear ip traffic

Related Commands	Command	Description
	show ip traffic	Displays IP traffic information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service, use the **clear ip wccp** command.

clear ip wccp [**vrf** *vrf-name*] {*service-number* | **web-cache**}

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies the VRF in which the service group needs to be created. If no VRF is specified, then the service number is created in the default global VRF. The <i>vrf-name</i> can be any case-sensitive alphanumeric string up to 32 characters.
<i>service-number</i>	Dynamic service identifier. The <i>service-number</i> range is from 1 to 255.
web-cache	Specifies the web-cache well-known service.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **clear ip wccp** command to clear the WCCP statistics.
This command does not require a license.

Examples

The following example shows how to clear the WCCP statistics for the web cache service:

```
switch(config)# clear ip wccp web-cache
```

Related Commands

Command	Description
feature wccp	Enables the WCCP feature.
ip wccp	Enables WCCP redirection for a service.
show ip wccp	Displays global statistics related to WCCP.

Send document comments to nexus7k-docfeedback@cisco.com

clear ipv6 adjacency statistics

To clear adjacency statistics, use the **clear ipv6 adjacency statistics** command.

clear ipv6 adjacency statistics

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example clears the adjacency statistics: switch# clear ipv6 adjacency statistics

Related Commands	Command	Description
	show ipv6 adjacency	Displays adjacency information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ipv6 eigrp accounting

To clear the prefix accounting information for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 processes, use the **clear ipv6 eigrp accounting** command.

clear ipv6 eigrp [*instance-tag*] **accounting** [**vrf** {*vrf-name* | *}]

Syntax Description

<i>instance-tag</i>	(Optional) Instance tag. 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 63 characters.
vrf <i>vrf-name</i>	(Optional) Name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear the EIGRP accounting information:

```
switch# clear ipv6 eigrp accounting
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ipv6 eigrp neighbors

To remove and reestablish the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 neighbor entries from the appropriate table, use the **clear ipv6 eigrp neighbors** command in EXEC mode.

```
clear ipv6 eigrp [instance-tag] neighbors [* | ipv6-address | interface-type interface-instance]
[soft] [vrf {vrf-name | *}]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Instance identifier. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
*	(Optional) Clears all neighbors.
<i>ipv6-address</i>	(Optional) Address of the neighbor. The format is A:B::C:D.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) CLI help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance. Specifying these arguments removes the specified interface type from the neighbor table that all entries learned through this interface. For more information about the interface syntax, use the question mark (?) online help function.
soft	(Optional) Specifies a soft reset for the neighbors.
vrf { <i>vrf-name</i> *}	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances. The VRF name is an alphanumeric string of up to 32 characters.

Defaults	Clears all instances if no instance is specified. Clears the default VRF if no VRF is specified.

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to clear all EIGRP entries for neighbors on Ethernet interface 2/1: switch# clear ipv6 eigrp vrf * neighbors ethernet 2/1

 `clear ipv6 eigrp neighbors`

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
<code>show ipv6 eigrp interfaces</code>	Displays information about interfaces configured for EIGRP.
<code>show ipv6 eigrp neighbors</code>	Displays the neighbors discovered by EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ipv6 eigrp route-map statistics redistribute

To clear statistics for routes redistributed into the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 topology table, use the **clear ipv6 eigrp route-map statistics redistribute** command.

```
clear ipv6 eigrp route-map statistics redistribute { bgp id | direct | eigrp id | isis id | ospfv3 id | rip 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 EIGRP.
isis	Clears policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
ospfv3	Clears policy statistics for the Open Shortest Path First (OSPF) version 3 protocol.
rip	Clears policy statistics for the Routing Information Protocol (RIP).
static	Clears policy statistics for IP static routes.
<i>id</i>	For the bgp keyword, the <i>id</i> 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. For the eigrp keyword, the <i>id</i> 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 NX-OS stores it internally as a string. For the isis keyword, the <i>id</i> is an IS-IS 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 NX-OS stores it internally as a string. For the ospf keyword, the <i>id</i> is 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i> *	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

 `clear ipv6 eigrp route-map statistics redistribute`

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear policy statistics for RIP:

```
switch# clear ipv6 eigrp route-map statistics redistribute rip 201
```

Related Commands

Command	Description
<code>show ipv6 eigrp route-map statistics</code>	Displays redistribution statistics for EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ipv6 eigrp redistribution

To clear redistribution information for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **clear ipv6 eigrp redistribution** command.

```
clear ipv6 eigrp redistribution [vrf {vrf-name | *}]
```

Syntax Description	vrf <i>vrf-name</i> * (Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.				
Defaults	None				
Command Modes	Any				
Supported User Roles	network-admin vdc-admin				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.2(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.2(1)	This command was introduced.
Release	Modification				
4.2(1)	This command was introduced.				
Usage Guidelines	This command requires the Enterprise Services license.				
Examples	The following example shows how to clear redistribution information: <pre>switch# clear ipv6 eigrp redistribution</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>feature eigrp</td><td>Enables the EIGRP feature.</td></tr></table>	Command	Description	feature eigrp	Enables the EIGRP feature.
Command	Description				
feature eigrp	Enables the EIGRP feature.				

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ipv6 eigrp traffic

To clear the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 traffic statistics, use the **clear ipv6 eigrp traffic** command.

clear ipv6 eigrp [*instance-tag*] **traffic** [**vrf** {*vrf-name* | *}]

Syntax Description

<i>instance-tag</i>	(Optional) Instance of EIGRP. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
vrf <i>vrf-name</i>	(Optional) Name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults

This command clears information for the default VRF if no VRF is specified.

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear the EIGRP traffic statistics:

```
switch# clear ipv6 eigrp traffic
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>type</i>	(Optional) Interface type. Use ? to see the list of supported interfaces.
	<i>number</i>	(Optional) Interface number. Use ? to see the range.
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	The following example clears ICMPv6 statistics: switch(config-if)# clear ipv6 icmp interface statistics	
Related Commands	Command	Description
	ipv6 icmp	Configures ICMPv6 on an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>type</i>	(Optional) Interface type. Use ? to see the list of supported interfaces.
<i>number</i>	(Optional) Interface number. Use ? to see the range.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example clears ND information:

```
switch(config-if)# clear ipv6 nd interface statistics  
N
```

Related Commands

Command	Description
ipv6 nd	Configures ICMPv6 ND on an interface.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>type</i>	(Optional) Interface type. Use ? to see the list of supported interfaces.
	<i>number</i>	(Optional) Interface number. Use ? to see the range.
	force-clear	(Optional) Clears the IPv6 neighbor cache without a refresh.
	vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.2(1)	Added force-clear keyword.
	4.0(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	The following example clears IPv6 neighbors: switch# clear ipv6 neighbor

Related Commands	Command	Description
	ipv6 nd	Configures ICMPv6 ND on an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ipv6 route

To clear individual routes from the unicast RIB, use the **clear ipv6 route** command.

clear ipv6 route [* | *addr* | *prefix*]] [**vrf** *vrf-name*]

Syntax Description

*	(Optional) Clears all routes.
<i>addr</i>	(Optional) Clears this route. The format is A:B::C:D.
<i>prefix</i>	(Optional) Clears this prefix. The format is A:B::C:D/length.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

Use the **clear ipv6 route** command to clear individual routes from the route table.



Note

The * keyword is severely disruptive to routing.

This command does not require a license.

Examples

The following example clears the individual route:

```
switch(config)# clear ipv6 route 2001:0DB8::/8
```

Related Commands

Command	Description
show ipv6 route	Displays entries in the route table.

Send document comments to nexus7k-docfeedback@cisco.com

clear ipv6 traffic

To clear IPv6 traffic information, use the **clear ipv6 traffic** command.

clear ipv6 traffic

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example clears the IPv6 traffic information: switch(config)# clear ip traffic

Related Commands	Command	Description
	show ipv6 traffic	Displays IPv6 traffic information.

Send document comments to nexus7k-docfeedback@cisco.com

clear isis adjacency

To clear adjacency information for Intermediate-System-to-Intermediate System (IS-IS), use the **clear isis adjacency** command.

clear isis [*instance-tag*] **adjacency** [* | *interface* | **system-id** *sid*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
*	(Optional) Clears all adjacency information for all interfaces.
<i>interface</i>	(Optional) An interface. Use ? to determine the supported interface types.
system-id <i>sid</i>	(Optional) Clears the adjacency information for this system ID. The <i>sid</i> format is XXXX.XXXX.XXXX.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear all the adjacency information:

```
switch# clear isis adjacency *
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear isis ip route-map statistics redistribute

To clear statistics for route redistribution for Intermediate-System-to-Intermediate System (IS-IS), use the **clear isis ip route-map statistics redistribute** command.

```
clear isis [instance-tag] ip route-map statistics redistribute { bgp id | direct | eigrp id | isis id |
ospf id | rip id | static } [vrf vrf-name]
```

Syntax Description	<i>instance-tag</i>	(Optional) Name of the IS-IS instance. Specify as an alphanumeric string.
	ip	(Optional) Clears statistics for IPv4.
	ipv6	(Optional) Clears statistics for IPv6.
	bgp	Clears statistics for the Border Gateway Protocol (BGP).
	direct	Clears statistics for directly connected routes only.
	eigrp	Clears statistics for the Enhanced Interior Gateway Protocol (EIGRP) routing protocol.
	isis	Clears statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
	ospf	Clears statistics for the Open Shortest Path First (OSPF) protocol.
	rip	Clears statistics for the Routing Information Protocol (RIP).
	static	Clears statistics for IP static routes.
	<i>id</i>	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 isis , eigrp , 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 NX-OS stores it internally as a string.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display policy statistics for redistributed routes:

```
switch# clear isis ip route-map statistics redistribute bgp
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

clear isis redistribution

To clear redistribution information for Intermediate-System-to-Intermediate System (IS-IS) , use the **clear isis redistribution** command.

```
clear isis [instance-tag] redistribution [vrf {vrf-name | all}]
```

Syntax Description	<i>instance-tag</i>	(Optional) Name of the IS-IS instance. Specify as an alphanumeric string.
	vrf <i>vrf-name</i> all	(Optional) Specifies a particular virtual routing and forwarding (VRF) instance. The VRF name is an alphanumeric string of up to 32 characters.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.2(1)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Examples	The following example shows how to clear redistribution information: switch# clear isis redistribution	
Related Commands	Command	Description
	feature isis	Enables the IS-IS feature.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear isis route-map statistics distribute

To clear statistics for route distribution between level-1 and level-2 areas for Intermediate-System-to-Intermediate System (IS-IS), use the **clear isis route-map statistics distribute** command.

```
clear isis [instance-tag] [ip | ipv6] route-map statistics distribute [level-1 | level-2] into [level-1 | level-2] [vrf vrf-name]
```

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
ip	(Optional) Clears statistics for IPv4.
ipv6	(Optional) Clears statistics for IPv6.
level-1	(Optional) Clears Level 1 distribution statistics.
level-2	(Optional) Clears Level 2 distribution statistics.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear the distribution information:

```
switch# clear isis route-map statistics distribute level-1 into level 2
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear isis statistics

To clear statistics for Intermediate-System-to-Intermediate System (IS-IS), use the **clear isis statistics** command.

clear isis [*instance-tag*] **statistics** [* | *interface*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
*	(Optional) Clears the statistics for all interfaces.
<i>interface</i>	(Optional) Interface name and interface number. Use ? to see a list of interfaces.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear the IS-IS statistics:

```
switch# clear isis statistics ethernet 7/45
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

clear isis traffic

To clear traffic statistics for Intermediate-System-to-Intermediate System (IS-IS), use the **clear isis traffic** command.

clear isis [*instance-tag*] **traffic** [* | *interface*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
*	(Optional) Clears the traffic statistics for all interfaces.
<i>interface</i>	(Optional) Interface name and interface number. Use ? to see a list of interfaces.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to clear the traffic statistics:

```
switch# clear isis traffic ethernet 7/45
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ospfv3 neighbor

To clear neighbor statistics and reset adjacencies for Open Shortest Path First version 3 (OSPFv3), use the **clear ospfv3 neighbor** command.

clear ospfv3 [*instance-tag*] **neighbor** { * | *neighbor-id* | *interface-type number* | **loopback** *number* | **port-channel** *number* } [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 32 characters.
*	Clears all neighbors.
<i>neighbor-id</i>	Specifies the Neighbor ID (as an IP address) of the neighbor to clear.
<i>interface-type number</i>	Specifies interface from which to clear all neighbors.
loopback <i>number</i>	Clears all neighbors on a loopback interface.
port-channel <i>number</i>	Clears all neighbors on a port-channel interface.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPFv3 virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string up to 32 characters, except “default” and “all”.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **clear ospfv3 neighbor** command to clear neighbor information from the **show ospfv3 neighbors** command. Use the *instance-tag* argument to clear the neighbor details from one OSPFv3 instance. If you do not use the *instance-tag* argument, Cisco NX-OS clears the neighbor details from all OSPFv3 instances. Use the **show ospfv3 neighbors** command to find the neighbor ID.

This command requires the Enterprise Services license.

Examples

The following example shows how to clear all OSPFv3 neighbor details for neighbor 192.0.2.1 for instance tag 201:

```
switch# clear ospfv3 201 neighbor 192.0.2.1
```


Send document comments to nexus7k-docfeedback@cisco.com

The following example shows how to clear all OSPFv3 neighbor details for all OSPFv3 instances:

```
switch# clear ospfv3 neighbor *
```

The following example shows how to clear all OSPFv3 neighbor details for all neighbors on Ethernet interface 1/2 for OSPFv3 instance 202:

```
switch# clear ospfv3 202 neighbor ethernet 1/2
```

Related Commands

Command	Description
<code>show ospfv3 neighbor</code>	Displays details for OSPFv3 neighbors including the neighbor ID.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ospfv3 policy statistics

To clear policy statistics for Open Shortest Path First version 3 (OSPFv3), use the **clear ospfv3 policy statistics** command.

```
clear ospfv3 [instance-tag] policy statistics {area area-id filter-list {in | out} | redistribute {bgp
autonomous-system | direct | eigrp id | isis id | rip id | static}} [vrf vrf-name]
```

Syntax	Description
<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 32 characters.
area	Clears policy statistics for an area.
<i>area-id</i>	Area ID as an integer or IP address.
filter-list	Specifies the policy statistics for filtered prefixes between OSPFv3 areas.
in	Filters prefixes sent into this OSPFv3 area.
out	Filters prefixes sent from this OSPFv3 area.
redistribution	Clears OSPFv3 route redistribution statistics.
bgp <i>autonomous-system</i>	Specifies the autonomous system number for the Border Gateway Protocol. Specify the autonomous system number as <i>x.y</i> , where the range is from 1 to 65535 for both <i>x</i> and <i>y</i> , or as a single integer, where the range is from 1 to 65535.
direct	Specifies directly connected routes.
eigrp <i>id</i>	Specifies the EIGRP instance. Specify the <i>id</i> argument as any alphanumeric string.
isis <i>id</i>	Specifies the Intermediate System to Intermediate System instance. Specify the <i>id</i> argument as any alphanumeric string.
rip <i>id</i>	Specifies the Routing Information Protocol instance. Specify the <i>id</i> argument as any alphanumeric string.
static	Specifies static routes.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPFv3 virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string up to 32 characters, except “default” and “all”.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **clear ospfv3 statistics** command to learn the policy statistics shown in the **show ospfv3 policy statistics** command. Use the *instance-tag* argument to clear the policy statistics from one OSPFv3 instance. If you do not specify the instance tag.

Cisco NX-OS clears the policy statistics from all OSPFv3 instances. Use the **show ospfv3 policy statistics** command to view the statistics that you are clearing.

This command requires the Enterprise Services license.

Examples

The following example shows how to clear all OSPFv3 policy statistics for area 99 inbound filtered routes for OSPFv3 201:

```
switch# clear ospfv3 201 policy statistics area 99 filter-list in
```

The following example shows how to clear all OSPFv3 policy statistics for all BGP redistributed routes for OSPFv3 202:

```
switch# clear ospfv3 202 policy statistics redistribute bgp
```

Related Commands

Command	Description
show ospfv3 policy statistics	Displays details for OSPFv3 policies.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear ospfv3 statistics

To clear Open Shortest Path First version 3 (OSPFv3) event statistics, use the **clear ospfv3 statistics** command.

clear ospfv3 [*instance-tag*] **statistics** [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 32 characters.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPFv3 virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string up to 32 characters, except “default” and “all”.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **clear ospfv3 statistics** command to clear the event statistics from one or more OSPFv3 instances. If you do not specify the *instance-tag* argument, Cisco NX-OS clears statistics from all OSPFv3 instances. Use the **show ospfv3 statistics** command to view the statistics that you are clearing.

This command requires the Enterprise Services license.

Examples

The following example shows how to clear all OSPFv3 event statistics:

```
switch# clear ospfv3 statistics
```

Related Commands

Command	Description
show ospfv3 statistics	Displays event statistics for OSPFv3.

Send document comments to nexus7k-docfeedback@cisco.com

clear ospfv3 traffic

To clear Open Shortest Path First version 3 (OSPFv3) traffic statistics, use the **clear ospfv3 traffic** command.

clear ospfv3 [*instance-tag*] **traffic** [**vrf** *vrf-name*]

Syntax Description	<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string of up to 32 characters.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the OSPFv3 virtual routing and forwarding instance (VRF). The <i>vrf-name</i> argument can be any alphanumeric string up to 32 characters, except “default” and “all”.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Use the clear ospfv3 traffic command to clear the traffic statistics from one or more OSPFv3 instances. If you do not specify the <i>instance-tag</i> argument, Cisco NX-OS clears traffic statistics from all OSPFv3 instances. Use the show ospfv3 traffic statistics command to view the statistics that you are clearing. This command requires the Enterprise Services license.	
Examples	The following example shows how to clear OSPFv3 traffic statistics for OSPFv3 100: switch# clear ospfv3 100 traffic	
Related Commands	Command	Description
	show ospfv3 traffic statistics	Displays OSPFv3 traffic statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear route-map pbr-statistics

To clear policy-based statistics for a route map, use the **clear route-map pbr statistics** command..

clear route-map *name* **pbr-statistics**

Syntax Description	<i>name</i>	Name of the route map. The name can be any alphanumeric string up to 63 characters.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Use the clear route-map pbr-statistics command to clear policy-based routing statistics enabled by the route-map pbr-statistics command. This command requires the Enterprise Services license.	
Examples	The following example shows how to clear the policy-base routing statistics for a route map: <pre>switch# clear route-map testmap pbr-statistics</pre>	
Related Commands	Command	Description
	route-map pbr-statistics	Enables policy-based routing statistics for a route map.

Send document comments to nexus7k-docfeedback@cisco.com

clear sockets statistics

To clear the socket statistics, use the **clear sockets statistics** command.

clear sockets statistics [**all** | **raw** | **raw6** | **tcp** | **tcp6** | **udp** | **udp6**]

Syntax Description	all	(Optional) Clears all the socket statistics.
	raw	(Optional) Clears the socket statistic for the raw IPv4 protocol s.
	raw6	(Optional) Clears the socket statistic for the raw IPv6 protocol s.
	tcp	(Optional) Clears the socket statistic for the TCP IPv4 protocol s.
	tcp6	(Optional) Clears the socket statistic for the TCP IPv6 protocol s.
	udp	(Optional) Clears the socket statistic for the UDP IPv4 protocol s.
	udp6	(Optional) Clears the socket statistic for the UDP IPv6 protocol s.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example shows how to clear the TCP socket statistics: switch# clear sockets statistics tcp

Related Commands	Command	Description
	show sockets statistics	Displays information about the socket statistics.
	show sockets client	Displays information about the socket client information.
	show sockets connection	Displays information about the socket connection.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

clear vrrp

To clear the Virtual Router Redundancy Protocol (VRRP) statistics, use the **clear vrrp** command.

clear vrrp { **statistics** | [**ipv4** | **vr id**] **interface** *if-number* }

Syntax Description	statistics	(Optional) Clears all VRRP statistics.
	ipv4	(Optional) Clears VRRP statistics on an interface.
	vr id	(Optional) Clears VRRP statistics in a VRRP group on an interface.
	interface <i>if-number</i>	(Optional) Clears VRRP statistics on an interface. Use ? to see a list of supported interfaces.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows how to clear VRRP statistics: switch(config)# clear vrrp

Related Commands	Command	Description
	feature vrrp	Enables the VRRP feature.
	clear vrrp	Clears VRRP statistics.

Send document comments to nexus7k-docfeedback@cisco.com

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 AS number.
	peers	Sets the peer AS numbers for a BGP confederation.
	<i>as-number</i>	The 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>.

Defaults	None

Command Modes	Router configuration mode Router VRF mode

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how configure the confederation identifier:

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

Related Commands	Command	Description
	show bgp	Displays information about BGP.

Send document comments to nexus7k-docfeedback@cisco.com



D Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter D.

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	<i>seconds</i>	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.
Defaults	The default value for <i>seconds</i> is four times the interval set by the hello-interval command.	
Command Modes	Virtual link configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

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.

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 Enterprise Services license.

Examples

The following 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
```

Related Commands

Command	Description
hello-interval (OSPF virtual link)	Interval between hello packets that Cisco NX-OS sends on the virtual link.
show ip ospf virtual-link	Displays OSPF-related information for a virtual link.

Send document comments to nexus7k-docfeedback@cisco.com

dead-interval (OSPFv3 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 version 3 (OSPFv3) 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

<i>seconds</i>	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.

Defaults

The default value for *seconds* is four times the interval set by the **hello-interval** command.

Command Modes

Virtual link configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **dead-interval** command in virtual link configuration mode to configure the dead interval advertised in OSPFv3 hello packets. This value must be the same for all networking devices on the virtual link.

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 ospfv3 virtual-links** command to verify the dead interval.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the OSPFv3 dead interval to 20 seconds:

```
switch(config)# ospfv3 201
switch(config-router)# area 99 virtual-link 192.0.2.4
switch(config-router-vlink)# dead-interval 20
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
hello-interval (OSPFv3 virtual link)	Interval between hello packets that Cisco NX-OS sends on the virtual link.
show ospfv3 virtual-link	Displays OSPFv3-related information for a virtual link.

Send document comments to nexus7k-docfeedback@cisco.com

default-information originate (EIGRP)

To generate a default route into the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-information originate** command in the appropriate configuration mode. 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 <i>map-name</i>	(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.

Defaults

Disabled

Command Modes

Address-family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
default-metric	Sets the metric for routes redistributed into EIGRP.
redistribute	Redistributes routes from other routing protocols into EIGRP.

Send document comments to nexus7k-docfeedback@cisco.com

default-information originate (IS-IS)

To control the origination of a default route, use the **default-information originate** command.

default-information originate [**always**] [**route-map** *name*]

Syntax Description

always	Always advertise the default route.
route-map <i>name</i>	Specifies the name of the routing rules route map to announce default routes. The name can be up to 63 characters.

Command Default

The default route is not redistributed into the IS-IS routing domain.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can force a default route into an IS-IS routing domain. Whenever you specifically configure redistribution of routes into an IS-IS routing domain, by default, the default route is not redistributed into the IS-IS routing domain. The **default-information originate route-map** command generates a default route into IS-IS, which can be controlled by a route map. You can use the route map to identify the level into which the default route is to be announced, and you can specify other filtering options configurable under a route map. You can use a route map to conditionally advertise the default route, depending on the existence of another route in the routing table of the router.

Examples

The following example shows how to always advertise the default route:

```
switch(config)# router isis TEST1
switch(config-router)# default-information originate always
switch(config-router)#
```

The following example shows how to specify a route map to conditionally advertise the default route:

```
switch(config)# router isis TEST1
switch(config-router)# default-information originate route-map CORE1
switch(config-router)#
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
exit	Exits the current configuration mode.
feature isis	Enables IS-IS on the router.
no	Negates a command or sets its defaults.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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 <i>map-name</i>	(Optional) Specifies to advertise the default route if the route map is satisfied. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.

Defaults Advertises the default route if the route is in the route table.

Command Modes Router configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(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 NX-OS 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 Enterprise Services license.

Examples The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config-router)# redistribute eigrp 108 route-map EigrpPolicy
switch(config-router)# default-information originate always
```

Related Commands

Command	Description
redistribute (OSPF)	Redistributes routes from one routing domain into OSPF.
route-map	Defines a filter policy for routes.

Send document comments to nexus7k-docfeedback@cisco.com

default-information originate (OSPFv3)

To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) 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 <i>map-name</i>	(Optional) Specifies to advertise the default route if the route map is satisfied. The <i>map-name</i> argument can be any alphanumeric string up to 63 characters.

Defaults

Advertises the default route if the route is in the route table.

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 OSPFv3 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 OSPFv3 routing domain.

Use the **route-map** keyword to filter redistributed routes so that Cisco NX-OS 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 Enterprise Services license.

Examples

This example shows how to configure the default route redistributed into the OSPFv3 routing domain for the Border Gateway Protocol (BGP):

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# router ospfv3 109  
switch(config-router)# redistribute bgp 108 route-map bgpPolicy  
switch(config-router)# address-family ipv6 unicast  
switch(config-router-af)# default-information originate always
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes routes from one routing domain into OSPFv3.
route-map	Defines a filter policy for routes.

Send document comments to nexus7k-docfeedback@cisco.com

default-information originate (RIP)

To generate a default route into the the Routing Information Protocol (RIP), use the **default-information originate** command in router address-family configuration mode. 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 <i>map-name</i>	(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.

Defaults

This command is disabled by default.

Command Modes

Router address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following 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
```

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>bandwidth</i>	Minimum bandwidth of the route in kilobits per second. The range is from 1 to 16777215. The default value is 100000.
<i>delay</i>	Route delay in tens of microseconds. The range is from 1 to 16777215. The default value is 100 (tens of microseconds).
<i>reliability</i>	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.
<i>loading</i>	Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100-percent loading). The default value is 1.
<i>mtu</i>	Minimum maximum transmission unit (MTU) size of the route in bytes. The range is from 1 to 4294967295. The default value is 1492.

Defaults

bandwidth: 100000
 delay: 100 (tens of microseconds)
 reliability: 255
 loading: 1
 MTU: 1500

Command Modes

Address-family configuration
 Router configuration
 Router VRF configuration

Supported User Roles

network-admin
 vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Changed the default value for MTU to 1492.

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 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.

Send document comments to nexus7k-docfeedback@cisco.com

This command requires the Enterprise Services license.

Examples

The following 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
```

Related Commands

Command	Description
redistribute	Redistributes routes from one routing domain into another routing domain.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>metric-value</i>	Default metric value appropriate for the specified routing protocol. The range is from 1 to 1677214.

Defaults

The metric for redistributed, connected, and static routes is set to 25.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
redistribute (OSPF)	Redistributes routes from another routing domain into OSPF.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

default-metric (OSPFv3)

To set default metric values for the Open Shortest Path First version 3 (OSPFv3) 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	<i>metric-value</i>	Default metric value appropriate for the specified routing protocol. The range is from 1 to 1677214.

Defaults	The metric for redistributed, connected, and static routes is set to 25.

Command Modes	Address-family configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 directly connected routes. A default metric helps to redistribute routes with incompatible metrics. Whenever external route metrics do not convert to an OSPFv3 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 Enterprise Services license.

Examples	This example shows how to configure OSPFv3 to redistribute RIP and BGP and set the default metric to 10:

```
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# default-metric 10
switch(config-router-af)# exit
switch(config-router)# redistribute rip 109 route-map FilterRip
switch(config-router)# redistribute bgp 4 route-map FilterBgp
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands**Command****Description**

redistribute (OSPFv3)	Redistributes routes from another routing domain into OSPFv3.

Send document comments to nexus7k-docfeedback@cisco.com

default-metric (RIP)

To set default metric values for the 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

<i>value</i>	Default metric value. The range is from 1 to 15.

Defaults

value: 1

Command Modes

Router address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 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.

This command does not require a license.

Examples

The following 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
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.

Send document comments to nexus7k-docfeedback@cisco.com

default-information originate	Generates a default route for routes redistributed into RIP.
redistribute	Redistributes routes from one routing domain into another routing domain.

Send document comments to nexus7k-docfeedback@cisco.com

delay minimum

To delay HSRP initialization after a reload or after an interface comes up, use the **forwarder preempt** 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	delay minimum <i>min-delay</i>	The 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 <i>reload-delay</i>	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 mode

Supported User Roles network-admin
VDC administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use **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 prevent HSRP state flapping.

This command does not require a license.

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 0
switch(config)# ip address 172.16.6.5 255.255.255.0
switch(config)# hsrp 1
switch(config)# delay minimum 3 reload 10
switch(config)# ip 172.16.6.100
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature hsrp	Enables HSRP configuration.

Send document comments to nexus7k-docfeedback@cisco.com

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 <i>up-time</i>	Delays the object track state change for an up condition. The range is from 0 to 180 seconds..
	down <i>down-time</i>	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	
Supported User Roles	network-admin VDC administrator	
Command History	Release	Modification
	4.2(4))	This command was introduced.
Usage Guidelines	Use delay command to delay when object tracking detects an up or down state change for a tracked object or track list. This delay helps prevent state flapping. This command does not require a license.	
Examples	This example shows how to configure the delay timer for a tracked object: <pre>switch(config)# configure terminal switch(config)# track 1 interface ethernet 1/2 line-protocol switch(config-track)# delay up 30 down 30</pre>	
Related Commands	Command	Description
	track	Configures a tracked object or track list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 reset to default, use the **no** form of this command.

distance *internal-distance external-distance*

no distance

Syntax Description	<i>internal-distance</i>	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.
	<i>external-distance</i>	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.

Defaults	<i>internal-distance</i> : 90
	<i>external-distance</i> : 170

Command Modes	Address-family configuration
	Router configuration
	Router VRF configuration

Supported User Roles	network-admin
	vdc-admin

Command History	Release	Modification
	4.0(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, the higher the value, the lower the 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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following 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
```

Related Commands

Command	Description
show ip eigrp	Displays information about the Enhanced Interior Gateway Routing Protocol (EIGRP) running on the router.

Send document comments to nexus7k-docfeedback@cisco.com

distance (IS-IS)

To define an administrative distance for routes that are inserted into the routing table, use the **distance** configuration mode command. To return the administrative distance to its default distance definition, use the **no** form of this command.

distance *value*

no distance

Syntax Description

<i>value</i>	Administrative distance. Range: 1 to 255. Default: 115.

Command Default

The default route is not redistributed into the IS-IS routing domain.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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, 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.

This command requires the Enterprise Services license.

Examples

The following example shows how to set the administrative distance to 90:.

```
switch(config)# router isis TEST1  
switch(config-router)# distance 90
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
net	Specifies the Network Entity Title (NET) for an IS-IS process.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>distance</i> Administrative distance for all routes local to this OSPF process. The range is from 1 to 255.	
Defaults	110	
Command Modes	Router configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following example shows how to set the distance to 200, making the route less reliable: <pre>switch(config)# router ospf 1 switch(config-router)# distance 200 switch(config-router)# router ospf 2 switch(config-router)# distance 20</pre>	

Send document comments to nexus7k-docfeedback@cisco.com

distance (OSPFv3)

To define the Open Shortest Path First version 3 (OSPFv3) route administrative distance, use the **distance** command. To restore the default, use the **no** form of this command.

distance *distance*

no distance

Syntax Description	<i>distance</i> Administrative distance for all routes local to this OSPFv3 process. The range is from 1 to 255.	
Defaults	110	
Command Modes	Address-family configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	This example shows how to set the distance to 200, making the route less reliable: switch(config)# router ospfv3 1 switch(config-router)# address-family ipv6 unicast switch(config-router-af)# distance 200	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

distance (RIP)

To define the administrative distance assigned to routes discovered by the the Routing Information Protocol (RIP), use the **distance** command in the router address-family configuration mode. 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

<i>admin-distance</i>	Administrative distance to be assigned to RIP routes. The range is from 0 to 255.

Defaults

admin-distance: 120

Command Modes

Router address-family configuration

Command History

Release	Modification
4.0(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 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 at all and should be ignored.

[Table 1-1](#) lists default administrative distances.

Table 1-1 Default Administrative Distances of Routing Protocols

Routing Protocols	Administrative Distance Value
Connected interface	0
Static route out an interface	0
Static route to next hop	1
EIGRP Summary Route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-1 **Default Administrative Distances of Routing Protocols (continued)**

Routing Protocols	Administrative Distance Value
Internal BGP	200
Unknown	255

This command does not require a license.

Examples

The following 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
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.
redistribute	Redistributes routes from one routing domain into RIP.

Send document comments to nexus7k-docfeedback@cisco.com

distribute

To distribute routes between specific IS-IS levels, use the **distribute** command. To return to the default setting, use the **no** form of this command.

distribute {level-1 | level-2} into {level-1 | level-2} {all | route-map name}

Syntax Description

level-1	Distributes the interarea routes into level-1 of this IS-IS instance.
level-2	Distributes the interarea routes into level-2 of this IS-IS instance.
into	Specifies from one level to another level.
all	Distributes all route levels.
route-map name	Prevents distribution of a specific route-map. The name can be any alphanumeric string up to 63 characters.

Command Default

The default route is not distributed into the IS-S routing domain. If enabled, IS-IS allows distribution of route between level-1 and level-2 such that optimal inter-area routing could be obtained.

This command requires the Enterprise Services license.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

level-1—Summarizes the IP address into the level-1 area. Only routes redistributed into Level 1 are summarized with the configured address and mask value.

level-2—Summarizes the IP address into the level-2 area. Routes learned by level-1 routing are summarized into the level-2 backbone with the configured address and mask value. Redistributed routes into level-2 IS-IS will be summarized also.

In IS-IS, all areas are stub areas, which means that no routing information is leaked from the backbone (level-2) into areas (level-1). Level-1-only routers use default routing to the closest level-1-level-2 router in their area. This command enables you to redistribute level-2 IP routes into level-1 areas. This redistribution enables level-1-only routers to pick the best path for an IP prefix to get out of the area. This is an IP-only feature, CLNS routing is still stub routing.

For more control and scalability, a distribute list or a route map can control which level-2 IP routes can be redistributed into level-1. This command allows large IS-IS-IP networks to use areas for better scalability.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example distributes level-1 routes into a level-2 network:

```
switch(config)# distribute level-1 into level-2
```

Send document comments to nexus7k-docfeedback@cisco.com



E Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter E.

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 reset to default, use the **no** form of this command.

ebgp multihop *ttl-value*

no ebgp multihop *ttl-value*

Syntax Description	<i>ttl-value</i> TTL value for eBGP multihop. The range is from 2 to 255. You must manually reset the BGP sessions after using this command.					
Defaults	None					
Command Modes	BGP neighbor configuration					
SupportedUserRoles	network-admin vdc-admin					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(1)	This command was introduced.
Release	Modification					
4.0(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.					

Send document comments to nexus7k-docfeedback@cisco.com

This command requires the Enterprise Services license.

Examples

The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

eigrp graceful-restart

To enable graceful restart for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **eigrp graceful-restart** command. To reset to default, use the **no** form of this command.

eigrp graceful-restart

no eigrp graceful restart

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes

- Address-family configuration
- Router configuration
- Router VRF configuration

SupportedUserRoles

- network-admin
- vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	Replaced by graceful-restart command.

Usage Guidelines

Use the **eigrp graceful-restart** command to allow EIGRP to remain in the data forwarding path through a process restart. This command is the same as the **nsf** command.

This command requires the Enterprise Services license.

Examples The following example shows how to enable graceful restart:

```
switch(config)# router eigrp 1  
switch(config-router)# eigrp graceful-restart
```

Related Commands	Command	Description
	graceful-restart	Enables graceful restart.
	timers nsf	Configures timers for nonstop forwarding and graceful restart.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Replaced by log-neighbor-changes command.

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 Enterprise Services license.

Examples

The following 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-neighbor-changes	Enables logging of EIGRP neighbor changes.
log-neighbor-warnings	Enables logging of EIGRP neighbor warnings.
log-adjacency-changes	Enables logging of EIGRP adjacency state changes.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>seconds</i> (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 Router configuration Router VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	Replaced by log-neighbor-warnings command.
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 Enterprise Services license.	
Examples	The following 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-neighbor-changes	Enables logging of EIGRP neighbor changes.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
log-neighbor-warnings	Enables logging of EIGRP neighbor warnings.
log-adjacency-changes	Enables logging of EIGRP adjacency state changes.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>ip-address</i>	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. 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.

Command Modes

Address-family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Replaced by router-id command.

Usage Guidelines

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 unique value for each router.

This command requires the Enterprise Services license.

Examples

The following 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
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 <i>map-name</i>	(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
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Replaced by stub command.

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 will 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(s) are advertised.

Send document comments to nexus7k-docfeedback@cisco.com

This command requires the Enterprise Services license.

Usage Guidelines

The following example shows how to configure the router as a receive-only neighbor:

```
switch(config)# router eigrp 1  
switch(config-router)# eigrp stub receive-only
```

Send document comments to nexus7k-docfeedback@cisco.com



F Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter F.

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.	
Defaults	Disabled	
Command Modes	Configuration mode	
SupportedUserRoles	network-admin VDC administrator	
Command History	Release	Modified
	4.0(1)	This command was introduced.
Usage Guidelines	You must enable the BGP feature before you can configure BGP. This command requires the Enterprise Services license.	

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to enable a BGP configuration:

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

Related Commands

Command	Description
show bgp	Displays BGP configuration information.
router bgp	Creates a BGP instance.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults	Disabled

Command Modes	Configuration mode

SupportedUserRoles	network-admin VDC administrator

Command History	Release	Modified
	4.0(1)	This command was introduced.

Usage Guidelines	You must enable the EIGRP feature before you can configure EIGRP. This command requires the Enterprise Services license.

Examples	The following example shows how to enable the EIGRP feature: <pre>switch(config)# feature eigrp</pre>

Related Commands	Command	Description
	show {ip ipv6} eigrp	Displays EIGRP configuration information.
	router eigrp	Creates a EIGRP instance.

Send document comments to nexus7k-docfeedback@cisco.com

feature glbp

To enable the Gateway Load Balancing Protocol (GLBP), use the **feature glbp** command. To disable GLBP, use the **no** form of this command.

feature glbp

no feature glbp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Supported User Roles

Network Administrator
VDC Administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must globally enable GLBP before you can configure any GLBP options or create a GLBP group. This command does not require a license.

Examples

The following example shows how to enable GLBP:

```
switch(config)# feature glbp
```

Related Commands

Command	Description
authentication	Configures an authentication string for the GLBP group.
forwarder preempt	Configures a gateway to take over as AVF for a GLBP group if it has a higher priority than the current AVF.
ip (GLBP)	Activates the GLBP group.
load-balancing	Specifies the load-balancing method used by the AVG of GLBP.
preempt	Configures the gateway to take over as AVG for a GLBP group if it has a higher priority than the current AVG.
priority	Sets the priority level of the gateway within a GLBP group.
show glbp	Displays GLBP information.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
timers	Configures the time between hello packets sent by the GLBP gateway and the time for which the virtual gateway and virtual forwarder information is considered valid.
timers redirect	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
track	Configures an interface to be tracked where the GLBP weighting changes are based on the state of the interface.
weighting	Specifies the initial weighting value of the GLBP gateway.
weighting track	Specifies a tracking object where the GLBP weighting changes are based on the availability of the object being tracked.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults

Disabled

Command Modes

Global configuration

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **feature hsrp** command to enter HSRP configuration mode and enable HSRP. This command does not require a license.

Examples

The following example shows how to enable HSRP on Ethernet interface 1/1:

```
switch# config t
switch(config)# feature hsrp
switch(config-hsrp)#
```

Related Commands

Command	Description
hsrp group	Creates and activates an HSRP group.
show hsrp	Displays HSRP information.

Send document comments to nexus7k-docfeedback@cisco.com

feature isis

To enable the Intermediate System to Intermediate System Protocol (IS-IS), use the **feature isis** command. To disable ISIS, use the **no** form of this command.

feature isis

no feature isis

Syntax Description	This command has no arguments or keywords.

Defaults	Disabled

Command Modes	Configuration mode

SupportedUserRoles	network-admin VDC administrator

Command History	Release	Modified
	4.0(1)	This command was introduced.

Usage Guidelines	You must enable the IS-IS feature before you can configure IS-IS. This command requires the Enterprise Services license.

Examples	The following example shows how to enable the IS-IS feature: <pre>switch(config)# feature isis</pre>

Related Commands	Command	Description
	show isis	Displays IS-IS configuration information.
	router isis	Creates an IS-IS instance.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults

Disabled

Command Modes

Configuration mode

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modified
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the OSPF feature before you can configure OSPF.
This command requires the Enterprise Services license.

Examples

The following example shows how to enable the OSPF feature:
`switch(config)# feature ospf`

Related Commands

Command	Description
show ospf	Displays OSPF configuration information.
router ospf	Creates an OSPF instance.

Send document comments to nexus7k-docfeedback@cisco.com

feature ospfv3

To enable the Open Shortest Path First version 3 Protocol(OSPFv3), use the **feature ospfv3** command. To disable OSPFv3, use the **no** form of this command.

feature ospfv3

no feature ospfv3

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Configuration mode

SupportedUserRoles

network-admin
VDC administrator

Command History

Release	Modified
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the OSPFv3 feature before you can configure OSPFv3. This command requires the Enterprise Services license.

Examples

The following example shows how to enable the OSPv3 feature:

```
switch(config)# feature ospfv3
```

Related Commands

Command	Description
show ospfv3	Displays OSPFv3 configuration information.
router ospfv3	Creates an OSPFv3 instance.

Send document comments to nexus7k-docfeedback@cisco.com

feature pbr

To enable the policy-based routing (PBR) feature, use the **feature pbr** command. To disable PBR, use the **no** form of this command.

feature pbr

no feature pbr

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Configuration mode

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modified
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the PBR feature before you can configure policy-based routing.
This command requires the Enterprise Services license.

Examples

The following example shows how to enable the PBR feature:

```
switch(config)# feature pbr
```

Related Commands

Command	Description
ip policy route-map	Assigns a policy-based route map to an interface.
show ip policy	Displays information about policy-based routing.

Send document comments to nexus7k-docfeedback@cisco.com

feature rip

To enable throttling 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.

Defaults

Disabled

Command Modes

Configuration mode

SupportedUserRoles

network-admin
VDC administrator

Command History

Release	Modified
4.0(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.

Examples

The following example shows how to enable the RIP feature:

```
switch(config)# feature rip
```

Related Commands

Command	Description
show rip	Displays RIP configuration information.
router rip	Creates a RIP instance.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults

Disabled

Command Modes

Configuration mode

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modified
4.0(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.

Examples

The following example shows how to enable the VRRP feature:

```
switch(config)# feature vrrp
```

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.
clear vrrp	Clears all the software counters for the specified virtual router.

Send document comments to nexus7k-docfeedback@cisco.com

feature wccp

To enable the Web Cache Communication Protocol (WCCP), use the **feature wccp** command. To disable WCCP, use the **no** form of this command.

feature wccp

no feature wccp

Syntax Description	This command has no arguments or keywords.

Defaults	Disabled

Command Modes	Configuration mode

SupportedUserRoles	network-admin vdc-admin

Command Historyr	Release	Modified
	4.2(1)	This command was introduced.

Usage Guidelines	You must enable the WCCP feature before you can configure WCCPv2. This command does not require a license.

Examples	The following example shows how to enable the WCCP feature:

```
switch(config)# feature wccp
switch(config)# show ip wccp
Global WCCP information:
  Router information:
    Router Identifier:          20.20.20.2
    Protocol Version:          2.0
```

Related Commands	Command	Description
	clear ip wccp	Clears all the software counters for WCCPv2.
	show running-config wccp	Displays the WCCPv2 configuration.
	show ip wccp	Displays the status of the WCCP service group.

Send document comments to nexus7k-docfeedback@cisco.com

flush-routes (OSPF)

To flush routes on a nongraceful controlled 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

None

Defaults

Disabled

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **flush-routes** command when the OSPF Graceful Restart feature is not enabled.

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 will not unregister and the OSPF routes will be stale. The OSPF routes are eventually removed from the unicast RIB after a timeout period. If OSPF comes back up in graceful restart mode, the routes will be refreshed in the unicast RIB.

This command requires the Enterprise Services license.

Examples

The following example shows how to flush routes for a nongraceful restart:

```
switch(config)# router ospf 202
switch(config-router)# flush-routes
```

Related Commands

Command	Description
graceful-restart	Enables OSPF Graceful Restart.

Send document comments to nexus7k-docfeedback@cisco.com

flush-routes (OSPFv3)

To flush routes on a nongraceful controlled restart for the Open Shortest Path First version 3 (OSPFv3) protocol, use the **flush-routes** command. To disable this feature, use the **no** form of this command.

flush-routes

no flush-routes

Syntax Description

None

Defaults

Disabled

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **flush-routes** command when the OSPFv3 Graceful Restart feature is not enabled.

This command causes OSPF to unregister from the unicast RIB when OSPFv3 shuts down. The unicast RIB removes all the routes associated with this ospf instance. If you do not configure the **flush-routes** command, OSPFv3 will not unregister and the OSPFv3 routes will be stale. The OSPFv3 routes are eventually removed from the unicast RIB after a timeout period. If OSPFv3 comes back up in graceful restart mode, the routes will be refreshed in the unicast RIB.

This command requires the Enterprise Services license.

Examples

This example shows how to flush routes for a nongraceful restart:

```
switch(config)# router ospfv3 202  
switch(config-router)# flush-routes
```

Related Commands

Command	Description
graceful-restart	Enables OSPFv3 Graceful Restart.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

forwarder preempt

To configure a gateway to take over as the active virtual forwarder (AVF) for a Gateway Load Balancing Protocol (GLBP) group if the current AVF falls below its low weighting threshold, use the **forwarder preempt** command. To disable this function, use the **no** form of this command.

forwarder preempt [**delay minimum** *seconds*]

no forwarder preempt [**delay minimum** *seconds*]

Syntax Description	delay minimum <i>seconds</i>	(Optional) Specifies a minimum number of seconds that the gateway delays before taking over the role of AVF. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default	Forwarder preemption is enabled with a default delay of 30 seconds.

Command Modes	GLBP configuration

Supported User Roles	network-admin VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example shows how to configure a gateway to preempt the current AVF when the current AVF falls below its low weighting threshold. If the gateway preempts the current AVF, it waits 60 seconds before taking over the role of the AVF. <pre>switch(config)# interface ethernet 1/1 switch(config-if)# glbp 2 switch(config-glbp)# forwarder preempt delay minimum 60</pre>

Related Commands	Command	Description
	glbp	Enters GLBP configuration mode and creates a GLBP group.



G Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter G.

glbp

To enter GLBP configuration mode and create a Gateway Load Balancing Protocol (GLBP) group, use the **glbp** command. To delete a GLBP group, use the **no** form of this command.

glbp *group*

no glbp *group*

Syntax Description	<i>group</i> GLBP group number. The range is from 0 to 1023.				
Defaults	None				
Command Modes	Interface configuration				
Supported User Roles	Network Administrator VDC Administrator				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
Usage Guidelines	Use the glbp command to enter GLBP configuration mode and create a GLBP group if the group does not exist.				

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

You must configure all GLBP options before you use the **ip** command to assign a virtual IP address and activate the GLBP group.

This command does not require a license.

Examples

The following example shows how to create GLBP group 10 on Ethernet interface 1/1:

```
switch(config)# interface ethernet 1/1  
switch(config-if)# glbp 10
```

Related Commands

Command	Description
ip (GLBP)	Configures a virtual IP address and activates the GLBP group.
show glbp	Displays GLBP information.

**Note**

You must configure extended hold timers on all GLBP gateways if you configure non-default extended hold timers. You can configure different extended holdtimer values on each GLBP gateway, based on the expected system switchover delays.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

graceful-restart (BGP)

To enable the graceful restart and the graceful restart helper capability, use the graceful-restart or the graceful-restart-helper router BGP configuration mode command. To disable graceful restart and the graceful restart helper capability, use the no form of this command.

graceful-restart [**restart-time** *restart-time* | **stalepath-time** *stalepath-time*]

graceful-restart-helper

no graceful-restart { **restart-time** *restart-time* | **stalepath-time** *stalepath-time* } |
graceful-restart-helper

Syntax Description

restart-time <i>restart-time</i>	(Optional) Sets the maximum time period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. Range: 1 to 3600. Default: 120.
stalepath-time <i>stalepath-time</i>	(Optional) Sets the maximum time period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. Range: 1 to 3600. Default: 300.
graceful-restart-helper	Enables the graceful restart helper capability.

Command Default

Graceful restart and graceful restart helper are enabled by default. The following default values are used when the **graceful-restart** command is entered without any keywords or arguments:

- *restart-time*: 120 seconds
- *stalepath-time*: 360 seconds



Note

Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Command Modes

Neighbor address-family configuration
Router bgp configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

The **graceful-restart** command is used to configure or disable the graceful restart capability on a router in a BGP network. If the graceful restart capability is enabled after a BGP session has been established, you will need to restart the session with a soft or hard reset.

The default timer values for this feature are optimal for most network deployments. We recommend that they are adjusted only by experienced network operators. When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message. If consecutive restart operations occur, routes (from a restarting router) that were previously marked as stale will be deleted.

The **graceful-restart-helper** command is used to configure the local BGP router to support the graceful restart of a remote BGP peer.

Examples

The following example shows how to enable the BGP graceful restart capability:

```
switch(config-router)# graceful-restart  
switch(config-router)#
```

The following example shows how to set the restart timer is set to 240 seconds:

```
switch(config-router)# graceful-restart restart-timer 240  
switch(config-router)#
```

Send document comments to nexus7k-docfeedback@cisco.com

graceful-restart (EIGRP)

To enable graceful restart for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **graceful-restart** command. To reset to default, use the **no** form of this command.

graceful-restart

no graceful restart

Syntax Description	This command has no arguments or keywords.

Defaults	Enabled

Command Modes	Address-family configuration Router configuration Router VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines	Use the graceful-restart command to allow EIGRP to remain in the data forwarding path through a process restart. This command requires the Enterprise Services license.

Examples	The following example shows how to enable graceful restart: switch(config) # router eigrp 1 switch(config-router) # graceful-restart

Related Commands	Command	Description
	timers nsf	Configures timers for nonstop forwarding and graceful restart.

Send document comments to nexus7k-docfeedback@cisco.com

graceful-restart (IS-IS)

To enable the graceful restart for an IS-IS process, use the graceful-restart configuration mode command. To disable graceful restart, use the no form of this command.

graceful-restart

no graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

Graceful restart is enabled by default.

Command Modes

Address-family configuration
Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **graceful-restart** command is used to configure or disable the graceful restart capability on a router in an IS-IS network. If the graceful restart capability is enabled after an IS-IS session has been established, you will need to restart the session with a soft or hard reset.

This command requires the Enterprise Services license.

Examples

The following example shows how to enable the graceful restart capability:

```
switch(config-router)# graceful-restart
switch(config-router)#
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Creates an IS-IS instance.

Send document comments to nexus7k-docfeedback@cisco.com

graceful-restart (OSPF)

To configure nonstop forwarding for Open Shortest Path First (OSPF), use the **graceful-restart** command. To disable this feature, use the **no** form of this command.

graceful-restart [*grace-period seconds* | **helper-disable** | **planned-only**]

no graceful-restart [*grace-period seconds* | **helper-disable** | **planned-only**]

Syntax Description	grace-period <i>seconds</i>	(Optional) Configures the maximum interval (in seconds) that another router should wait for this router to gracefully restart. The range is from 5 to 1800.
	helper-disable	(Optional) Disables helper mode. The router will not participate in the graceful restart of a neighbor router.
	planned-only	(Optional) Enables graceful restart for controlled restarts only.

Defaults	Enabled by default. Grace period: 60 seconds

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the graceful-restart command to allow OSPF to remain in the data forwarding path through a process restart. Set the grace period long enough to allow a typical reboot cycle for Cisco NX-OS. Do not set the grace period too long or your network will be relying on old route information. This command requires the Enterprise Services license.

Examples	The following example shows how to configure a graceful restart to occur only for a planned restart: <pre>switch(config)# router ospf 202 switch(config-router)# graceful-restart grace-period 300 planned-only</pre>

Related Commands	Command	Description
	flush-routes	Flushes routes on a nongraceful controlled restart.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

graceful-restart (OSPFv3)

To configure nonstop forwarding for Open Shortest Path First version 3 (OSPFv3), use the **graceful-restart** command. To disable this feature, use the **no** form of this command.

graceful-restart [*grace-period seconds* | **helper-disable** | **planned-only**]

no graceful-restart [*grace-period seconds* | **helper-disable** | **planned-only**]

Syntax Description

grace-period <i>seconds</i>	(Optional) Configures the maximum interval (in seconds) that another router should wait for this router to gracefully restart. The range is from 5 to 1800.
helper-disable	(Optional) Disables helper mode. The router will not participate in the graceful restart of a neighbor router.
planned-only	(Optional) Enables graceful restart for controlled restarts only.

Defaults

Enabled by default. Grace period: 60 seconds

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **graceful-restart** command to allow OSPFv3 to remain in the data forwarding path through a process restart. Set the grace period long enough to allow a typical reboot cycle for Cisco NX-OS. Do not set the grace period too long or your network will be relying on old route information.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a graceful restart to occur only for a planned restart:

```
switch(config)# router ospfv3 202
switch(config-router)# graceful-restart grace-period 300 planned-only
```

Related Commands

Command	Description
flush-routes	Flushes routes on a nongraceful controlled restart.

Send document comments to nexus7k-docfeedback@cisco.com

graceful-restart t3 manual

To configure the time that Intermediate-System-to-Intermediate System (IS-IS) announces as the adjacency remaining time in its hello message when IS-IS acknowledges a peer restart, use the **graceful-restart t3 manual** command. To revert to the default setting, use the **no** form of this command.

graceful-restart t3 manual *time*

no graceful-restart t3 manual

Syntax Description	<i>time</i> Time in seconds. The range is from 30 to 65535.						
Command Default	60 seconds						
Command Modes	Router configuration VRF configuration						
Supported User Roles	network-admin vdc-admin						
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.1(2)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.1(2)	This command was introduced.		
Release	Modification						
4.1(2)	This command was introduced.						
Usage Guidelines	Use the graceful-restart t3 manual command to set the T3 timer, as defined in RFC 3847. This command requires the Enterprise Services license.						
Examples	The following example shows how to set the T3 timer: switch(config-router)# graceful-restart t3 manual 90 switch(config-router)#						
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Creates an IS-IS instance.</td></tr></table>	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Creates an IS-IS instance.
Command	Description						
feature isis	Enables IS-IS on the router.						
router isis	Creates an IS-IS instance.						

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com



H Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter H.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

hardware forwarding dynamic-allocation

To enable or disable dynamic TCAM block allocation in the Forwarding Information Base (FIB), use the **hardware forwarding dynamic-allocation** command.

hardware forwarding dynamic-allocation {enable | disable}

Syntax Description

enable	Enables dynamic TCAM allocation.
disable	Disables dynamic TCAM allocation.

Defaults

Enabled

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **hardware forwarding dynamic-allocation enable** command to reallocate unused blocks in the FIB.

Use the **hardware forwarding dynamic-allocation disable** command to disable the dynamic TCAM allocation. This command returns the TCAM to the default allocation if there are no routes in the reallocated blocks.

This command does not require a license.

Examples

The following example shows how to enable dynamic TCAM allocation:

```
switch(config)# hardware forwarding dynamic-allocation enable
```

Related Commands

Command	Description
show hardware forwarding dynamic-allocation	Displays information about dynamic TCAM allocation for each module.

Send document comments to nexus7k-docfeedback@cisco.com

hardware ip verify

To configure IP packet verification, use the **hardware ip verify** command. To disable IP packet verification, use the **no** form of this command.

hardware ip verify {checksum | fragment | protocol | tcp tiny-frag | version}

no hardware ip verify {checksum | fragment}

Syntax Description	checksum	Drops IPv4 or IPv6 packets if the checksum is invalid
	fragment	Drops IPv4 or IPv6 packets if the packet fragment has a nonzero offset and the DF bit is active.
	protocol	Drops IPv4 or IPv6 packets if the packet fragment has an invalid IP protocol number.
	tcp tiny-frag	Drops IPv4 packets if the IP fragment offset is 1, or if the IP fragment offset is 0 and the IP payload length is less than 16.
	version	Drops IPv4 packets if the ethertype is not set to 4 (IPv4).

Defaults	All address tests enabled.

Command Modes	Global configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.1(3)	This command was introduced.
	4.2(2)	Added protocol keyword.

Usage Guidelines	Use the hardware ip verify command to configure packet verification tests on IPv4 and IPv6 packets based on checksum or fragments.

This command replaces the **platform ip verify** command.

This command does not require a license.

Examples	This example shows how to drop fragmented IPv4 or IPv6 packets:

```
switch(config)# hardware ip verify fragment
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
hardware ip verify length	Configures IPv4 packet verification checks based on length.
hardware ipv6 verify	Configures IPv6 packet verification.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

Send document comments to nexus7k-docfeedback@cisco.com

hardware ip verify address

To enable packet verification tests on IP addresses, use the **hardware ip verify address** command. To disable packet verification tests, use the **no** form of this command.

hardware ip verify address { **destination zero** | **identical** | **reserved** | **source** { **broadcast** | **multicast** } }

no hardware ip verify address { **destination zero** | **identical** | **reserved** | **source** { **broadcast** | **multicast** } }

Syntax Description

destination zero	Drops IP packets if the destination IPv4 address is 0.0.0.0 or if the IPv6 address is ::.
identical	Drops IP packets if the source IPv4 or IPv6 address is identical to the destination IPv4 or IPv6 address.
reserved	Drops IP packets if the IPv4 address is in the 127.x.x.x range or if the IPv6 address is in the ::1 range.
source	Drops IP packets based on the IP source address
broadcast	Drops IP packets if the IP source address is 255.255.255.255
multicast	Drops IP packets if the IPv4 source address is in the 224.x.x.x range or if the IPv6 source address is in the FF00::/8 range.

Defaults

All address tests enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Use the **hardware ip verify address** command to configure packet verification tests on IPv4 and IPv6 packets based on addresses.

This command replaces the **platform ip verify address** command

This command does not require a license.

Examples

This example shows how to drop broadcast IPv4 packets:

```
switch(config)# hardware ip verify address source broadcast
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	hardware ip verify	Configures IPv4 and IPv6 packet verification checks based on checksum or fragments.
	hardware ip verify length	Configures IPv4 packet verification checks based on length.
	hardware ipv6 verify	Configures IPv6 packet verification.
	show hardware forwarding ip verify	Displays information about IP packet verification checks.

Send document comments to nexus7k-docfeedback@cisco.com

hardware ip verify length

To configure IPv4 packet verification tests based on packet length, use the **hardware ip verify length** command. To disable the tests, use the **no** form of this command.

hardware ip verify length { **consistent** | **maximum** { **max-frag** | **max-tcp** | **udp** } | **minimum** }

no hardware ip verify length { **consistent** | **maximum** { **max-frag** | **max-tcp** | **udp** } | **minimum** }

Syntax Description	
consistent	Drops IPv4 packets where the Ethernet frame size is greater than or equal to the IP packet length plus the Ethernet header.
maximum { max-frag max-tcp udp }	Drops IPv4 packets based on the following: • max-frag—Drops IP packets if the maximum fragment offset is greater than 65536. • max-tcp—Drops IP packets if the TCP length is greater than the IP payload length. • udp—Drops IP packets if the IP payload length is less than the UDP packet length.
minimum	Drops IP packets if the Ethernet frame length is less than the IP packet length plus four octets (the CRC length).

Defaults	All address tests enabled.

Command Modes	Global configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines	Use the hardware ip verify length command to configure packet verification tests on IPv4 and IPv6 packets based on packet length. This command replaces the platform ip verify length command. This command does not require a license.

Examples	This example shows how to drop minimum-length IPv4 packets: <pre>switch(config)# hardware ip verify length minimum</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	hardware ip verify	Configures IPv4 packet verification checks based on checksum or fragments.
	hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
	hardware ipv6 verify	Configures IPv6 packet verification.
	show hardware forwarding ip verify	Displays information about IP packet verification checks.

Send document comments to nexus7k-docfeedback@cisco.com

hardware ipv6 verify

To configure IPv6 packet verification tests, use the **hardware ipv6 verify** command. To disable the tests, use the **no** form of this command.

hardware ipv6 verify {length {consistent | maximum {max-frag | max-tcp | udp} | tcp tiny-frag | version}

no hardware ip verify {checksum | fragment}

Syntax Description	
length	Drops IPv6 packets based on length.
consistent	Drops IPv6 packets where the Ethernet frame size is greater than or equal to the IPv6 packet length plus the Ethernet header.
maximum {max-frag max-tcp udp}	Drops IPv6 packets based on the following: • max-frag—Drops IPv6 packets if the formula (IPv6 Payload Length – IPv6 Extension Header Bytes) + (Fragment Offset * 8) is greater than 65536. • max-tcp—Drops IPv6 packets if the TCP length is greater than the IP payload length. • udp—Drops IPv6 packets if the IP payload length is less than the UDP packet length.
tcp tiny-frag	Drops IPv6 packets if the IP fragment offset is 1, or if the IPv6 fragment offset is 0 and the IPv6 payload length is less than 16.
version	Drops IPv6 packets if the ethertype is not set to 6 (IPv6).

Defaults	All address tests enabled.

Command Modes	Global configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines

Use the **hardware ipv6 verify** command to configure packet verification tests on IPv6 packets.

This command replaces the **platform ipv6 verify** command.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to drop all IPv4 packets:

```
switch(config)# hardware ipv6 verify version
```

Related Commands

Command	Description
hardware ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
hardware ip verify length	Configures IPv4 packet verification checks based on length.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

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, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description

<i>seconds</i>	The 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.

Defaults

10 second.

Command Modes

Virtual link configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to configure the hello interval to 15 seconds:

```
switch(config)# router ospf 202  
switch(config-router)# ip ospf area 99 virtual-link 192.0.2.4  
switch(config-router-vlink)# hello-interval 15
```

Related Commands

Command	Description
dead-interval (virtual link)	Sets the time period to declare a neighbor as down if the local device receives no hello packets.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

hello-interval (OSPFv3 virtual link)

To specify the interval between hello packets that Cisco NX-OS sends on an Open Shortest Path First version 3 (OSPFv3) virtual link, use the **hello-interval** command. To return to the default, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description	<i>seconds</i>	The 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.

Defaults	10 second.

Command Modes	Virtual link configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the hello-interval command in virtual link configuration mode to set the hello interval for OSPFv3 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 Enterprise Services license.

Examples	This example shows how to configure the hello interval to 15 seconds:

```
switch(config)# router ospfv3 202
switch(config-router)# ipv6 ospfv3 area 99 virtual-link 192.0.2.4
switch(config-router-vlink)# hello-interval 15
```

Related Commands	Command	Description
	dead-interval (OSPFv3 virtual link)	Sets the time period to declare a neighbor as down if the local device receives no hello packets.

Send document comments to nexus7k-docfeedback@cisco.com

hostname dynamic

To enable the exchange of the dynamic host name for IS-IS, use the **hostname dynamic** configuration mode command. To disable the exchange of the dynamic host name for IS-IS, use the **no** form of this command

hostname *name*

no hostname *name*

Syntax Description This command has no arguments or keywords.

Command Default Dynamic host name is disabled by default.

Command Modes Router configuration
VRF configuration

Supported User Roles network-admin
vdc-admin

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines The **hostname dynamic** command allows you to enable the IS-IS routers to flood their host name to system ID mapping information across the IS-IS network.
This command requires the Enterprise Services license.

Examples The following example shows how to enable the exchange of the dynamic host name for IS-IS:

```
switch(config-router)# hostname dynamic
switch(config-router)#
```

The following example shows how to disable the exchange of the dynamic host name for IS-IS:

```
switch(config-router)# no hostname dynamic
switch(config-router)#
```

Command	Description
exit	Exits the current configuration mode.
feature isis	Enables IS-IS on the router.
no	Negates a command or sets its defaults.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
router isis	Enables IS-IS.
show isis hostname	Displays the IS-IS dynamic host name exchange information

Send document comments to nexus7k-docfeedback@cisco.com

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

<i>group-number</i>	The 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	Sets the HSRP group for IPv4.

Defaults

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Added the IPv4 keyword.

Usage Guidelines

You must globally enable HSRP before you can configure any HSRP options or create an HSRP group. This command does not require a license.

Examples

This example shows how to create and activate an HSRP group:

```
switch# configure t
switch(config)# interface ethernet 0
switch(config-if)# ip address 172.16.6.5 255.255.255.0
switch(config-if)# hsrp 1
switch(config-if-hsrp)#
```

Related Commands

Command	Description
feature hsrp	Enables HSRP configuration.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
show hsrp	Displays HSRP information.
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

Send document comments to nexus7k-docfeedback@cisco.com

hsrp timers extended-hold

To enable extended hold timers for the Hot Standby Router Protocol (HSRP), use the **hsrp timers extended-hold** command. To revert to default, use the **no** form of this command.

hsrp timers extended-hold *timer*

no hsrp timers extended-hold

Syntax Description	<i>timer</i> (Optional) Extended hold time, in seconds. The range is from 10 to 255.	
Defaults	10 seconds	
Command Modes	Global configuration	
Supported User Roles	Network Administrator VDC Administrator	
Command History	Release	Modification
	4.2(1)	This command was introduced.
Usage Guidelines	Use the hsrp timers extended-hold command to configure extended Non-stop Forwarding (NSF) support for HSRP.	
 Note	You must configure extended hold timers on all HSRP routers if you configure non-default extended hold timers. You can configure different extended hold timer values on each HSRP router, based on the expected system switchover delays.	
	This command does not require a license.	
Examples	The following example shows how to configure the extended hold time for HSRP: switch(config)# hsrp timers extended-hold 30	
Related Commands	Command	Description
	feature hsrp	Enables the HSRP feature.
	show hsrp	Displays HSRP information.

Send document comments to nexus7k-docfeedback@cisco.com



I Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter I.

ip (GLBP)

To activate the Gateway Load Balancing Protocol (GLBP) for a group, use the **ip** command. To disable GLBP in the group, use the **no ip** form of this command.

ip [*ip-address* [**secondary**]]

no ip [*ip-address* [**secondary**]]

Syntax Description	<i>ip-address</i>	(Optional) Virtual IP address for the GLBP group. The IP address must be in the same subnet as the interface IP address.
	secondary	(Optional) Indicates that the IP address is a secondary GLBP virtual address.
Defaults	Disabled	
Command Modes	GLBP configuration	
Supported User Roles	Network Administrator VDC Administrator	
Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Use the **ip** command to activate GLBP on the configured interface. If you configure a virtual IP address, that address is the designated virtual IP address for the entire GLBP group. If you do not configure a virtual IP address, the gateway learns the virtual IP address from another gateway in the same GLBP group. To allow GLBP 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 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 GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP 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 GLBP options before you use the **ip** command to assign a virtual IP address and activate the GLBP group.

This command does not require a license.

Examples

The following example shows how to activate GLBP for group 10 on Ethernet interface 1/1. The virtual IP address used by the GLBP group is set to 192.0.2.10.

```
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 192.0.2.32 255.255.255.0
switch(config-if)# glbp 10
switch(config-glbp)# ip 192.0.2.10
```

The following example shows how to activate GLBP for group 10 on Ethernet interface 2/1. The virtual IP address used by the GLBP group will be learned from another gateway configured to be in the same GLBP group.

```
switch(config)# interface ethernet 2/1
switch(config-if)# glbp 10
switch(config-glbp)# ip
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
show glbp	Displays GLBP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 [*ip-address* [**secondary**]]

no ip [*ip-address* [**secondary**]]

Syntax Description	<i>ip-address</i>	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.
	secondary	(Optional) Indicates that the IP address is a secondary HSRP virtual address.

Defaults	Disabled

Command Modes	HSRP configuration

Supported User Roles	network-admin VDC administrator

Command History	Release	Modification
	4.0(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. 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 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.

Send document comments to nexus7k-docfeedback@cisco.com


Note

You must configure all HSRP options before you use the **ip** command to assign a virtual IP address and activate the HSRP group. This helps you to 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

This command does not require a license.

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# config t
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 192.0.2.32 255.255.255.0
switch(config-if)# hsrp 10
switch(config-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)# hsrp 10
switch(config-hsrp)# ip
```

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# config t
switch(config)# interface ethernet 1/1
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 HSRP configuration.
show hsrp	Displays HSRP information.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>ip-address</i> IPv4 address, in A.B.C.D format. <i>mac-address</i> 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							
Defaults	None							
Command Modes	Interface configuration							
SupportedUserRoles	network-admin vdc-admin							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>4.2(1)</td><td>Support added for multicast static MAC addresses.</td></tr></table>		Release	Modification	4.0(1)	This command was introduced.	4.2(1)	Support added for multicast static MAC addresses.
Release	Modification							
4.0(1)	This command was introduced.							
4.2(1)	Support added for multicast static MAC addresses.							
Usage Guidelines	This command does not require a license.							
Examples	This example shows how to configure a static ARP entry on interface Ethernet 2/1: <pre>switch(config)# interface ethernet 1/2 switch(config-if)# ip arp 192.0.2.1 0150.5a03.efab</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip arp</td><td>Displays ARP entries.</td></tr></table>		Command	Description	show ip arp	Displays ARP entries.		
Command	Description							
show ip arp	Displays ARP entries.							

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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.

Defaults

Enabled.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to disable gratuitous ARP request on interface Ethernet 2/1:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip arp request
```

Related Commands

Command	Description
ip arp	Configures a static ARP entry.

Send document comments to nexus7k-docfeedback@cisco.com

ip as-path access-list

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

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

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

Syntax Description	<i>name</i>	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 <i>regex</i> argument.
	permit	Allows packets with AS numbers that match the <i>regex</i> argument
	<i>regex</i>	A regular expression to match BGP AS paths. See the <i>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2</i> at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/fundamentals/configuration/guide2/fun_nx-os_book.html

Defaults	None

Command Modes	Global configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

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
```

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>name-of-chain</i>	Group of keys that are valid.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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)# ip authentication key-chain eigrp 209 trees
```

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
md5	Specifies Message Digest 5 (MD5) authentication.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following 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)# ip authentication mode eigrp 209 md5
```

Related Commands

Command	Description
authentication mode (EIGRP)	Configures 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.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	<i>bandwidth</i>	Bandwidth value. The range is from 1 to 2,560,000,000 kilobits.
Defaults	None	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Examples	The following example shows how to configure EIGRP to use a bandwidth metric of 10000 in autonomous system 209: <pre>switch(config)# router eigrp 209 switch(config-router)# interface ethernet 2/1 switch(config-if)# ip bandwidth eigrp 209 10000</pre>	
Related Commands	Command	Description
	ip bandwidth-percent eigrp	Sets the percent of the interface bandwidth that EIGRP can use.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>percent</i>	Percentage of bandwidth that EIGRP may use.

Defaults

percent: 50

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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)# ip bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
ip bandwidth eigrp	Sets the EIGRP bandwidth value for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

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** } *regex*

no ip community-list expanded *list-name*

Syntax Description

standard <i>list-name</i>	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
<i>aa:nn</i>	(Optional) 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	(Optional) 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	(Optional) 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	(Optional) 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	(Optional) 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.

Send document comments to nexus7k-docfeedback@cisco.com

expanded <i>list-name</i>	Configures a named expanded community list.
<i>regexp</i>	Regular expression that is used to specify a pattern to match against an input string. See the <i>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2</i> at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/fundamentals/configuration/guide2/fun_nx-os_book.html
	
Note	Regular expressions can be used with expanded community lists only.

Defaults

Community exchange is not enabled by default.

Command Modes

Global configuration (config)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 trailing 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 address-family configuration mode to enable 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 trailing communities that exceed the limit are not processed or saved to the running configuration file.

Send document comments to nexus7k-docfeedback@cisco.com

You can configure up to 32 communities.

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 longest construct 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 will match 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.

This command does not require a license.

Examples

In the following example, a standard community list is configured that routes with this community are advertised to all peers (internal and external):

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

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

- 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 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 following example, a standard community list is configured to deny 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
```

In the following example, a named standard community list is configured 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)#
```

In the following example, an expanded community list is configured that will deny 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)#
```

Send document comments to nexus7k-docfeedback@cisco.com

In the following example, a named expanded community list configured 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]_  
switch(config)#
```

Related Commands

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

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	<i>seconds</i>	Throughput delay, in tens of microseconds. The range is from 1 to 16777215.

Defaults	100 (10-microsecond units).

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following 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)# 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.

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 "exploded" as a 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 will be exploded as broadcasts 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 will be 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 security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to enable forwarding of IP directed broadcasts on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip directed-broadcast
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
prefix-list <i>list-name</i>	Specifies the name of an IP prefix list to filter EIGRP routes.
route-map <i>map-name</i>	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.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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)# ip distribute-list eigrp 209 route-map InputFilter in
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip domain-list

To configure the IP domain list, use the **ip domain-list** command. To disable the IP domain list, use the **no** form of the command.

ip domain-list *domain-name* [**use-vrf** *name*]

no ip domain-list *domain-name* [**use-vrf** *name*]

Syntax Description	domain-list	Specifies the domain name for the IP domain list. The name can be any case-sensitive alphanumeric string up to 63 characters.
	use-vrf <i>name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain domain name for the IP domain list. The name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults None

Command Modes Global configuration
VRF context configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **ip domain-list** command to configure additional domain names for the device. Use the **vrf context** command to enter the VRF context mode to configure additional domain names for a particular VRF.

This command does not require a license.

Examples The following example configures the IP domain list for the default VRF.

```
switch# config terminal
switch(config)# ip domain-list Mysite.com
```

The following example configures the IP domain list for the management VRF.

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-list Mysite.com
```


Send document comments to nexus7k-docfeedback@cisco.com

The following example configures the IP domain list for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF.

```
switch# config terminal
switch(config)# ip domain-list Mysite.com use-vrf management
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

Send document comments to nexus7k-docfeedback@cisco.com

ip domain-lookup

To enable the Domain Name Server (DNS) lookup feature, use the **ip domain-lookup** command. Use the **no** form of this command to disable this feature.

ip domain-lookup

no ip domain-lookup

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip domain-lookup** command to enable DNS.

This command does not require a license.

Examples

The following example configures a DNS server lookup feature.

```
switch# config terminal  
switch(config)# ip domain-lookup
```

Related Commands

Command	Description
show hosts	Displays information about the DNS.

Send document comments to nexus7k-docfeedback@cisco.com

ip domain-name

To configure a domain name, use the **ip domain-name** command. To delete a domain name, use the **no** form of the command.

ip domain-name *domain-name* [**use-vrf** *name*]

no ip domain-name *domain-name* [**use-vrf** *name*]

Syntax Description	domain-name	Specifies the domain name. The name can be any case-sensitive alphanumeric string up to 63 characters.
	use-vrf <i>name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name. The name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Global configuration VRF context configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ip domain-name command to configure the domain name for the device. Use the vrf context command to enter the VRF context mode to configure the domain name for a particular VRF. This command does not require a license.

Examples	The following example configures the IP domain name for the default VRF.

```
switch# config terminal
switch(config)# ip domain-name Mysite.com
```

The following example configures the IP domain name for the management VRF.

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-name Mysite.com
```

The following example configures the IP domain name for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF.

Send document comments to nexus7k-docfeedback@cisco.com

```
switch# config terminal
switch(config)# ip domain-name Mysite.com use-vrf management
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>instance-tag</i> Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.	
Defaults	None	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following example shows how to disable EIGRP on an interface: <pre>switch(config)# router eigrp 201 switch(config-router)# interface ethernet 2/1 switch(config-if)# ip eigrp 201 shutdown</pre>	
Related Commands	Command	Description
	ip passive-interface eigrp	Configures an instance of EIGRP.
	router eigrp	Configures an instance of EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 <i>list-name</i>	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.
<i>aa4:nn</i>	(Optional) 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 <i>list-name</i>	Configures a named expanded extended community list.
<i>regexp</i>	Regular expression that is used to specify a pattern to match against an input string. See the <i>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2</i> at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/fundamentals/configuration/guide2/fun_nx-os_book.html
 Note	Regular expressions can be used with expanded extended community lists only.

Defaults

Community exchange is not enabled by default.

Command Modes

Global configuration

Send document comments to nexus7k-docfeedback@cisco.com

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.2(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 address-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 longest construct 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 will match 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.

This command does not require a license.

Examples

The following 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.

The following example shows a logical AND condition:

```
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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	<i>seconds</i>	Hello interval (in seconds). The range is from 1 to 65535.
Defaults	5 seconds	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Examples	The following example shows how to set the hello interval to 10 seconds for the interface: <pre>switch(config)# router eigrp 1 switch(config-router)# interface ethernet 2/1 switch(config-if)# ip hello-interval eigrp 1 10</pre>	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>seconds</i>	Hold time (in seconds). The range is from 1 to 65535.

Defaults

15 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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)# ip hold-time eigrp 209 40
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
ip hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process designated by an autonomous system number.

Send document comments to nexus7k-docfeedback@cisco.com

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache, use the **ip host** command. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host *name address1* [*address2... address6*]

no ip host *name address1* [*address2... address6*]

Syntax Description

<i>name</i>	Host name. The <i>name</i> can be any case-sensitive alphanumeric string up to 80 characters.
<i>address1</i>	IPv4 address in the x.x.x.x format.
<i>address2 ...address6</i>	(Optional) Up to five additional IPv4 addresses in the x.x.x.x format.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip host** command to add a static host name to DNS.
This command does not require a license.

Examples

The following example shows how to configure a static host name:

```
switch(config)# ip host mycompany.com 192.0.2.1
```

Related Commands

Command	Description
ipv6 host	Configures a static host name in the DNS database.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip load-sharing address

To configure the load-sharing algorithm used by the unicast 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 destination address and port.
	source-destination	Sets the load-sharing algorithm based on source and destination address.
	port source-destination	(Optional) Sets the load-sharing algorithm based on source and destination address and port address.
	universal-id <i>seed</i>	(Optional) Sets the random seed for the load sharing hash algorithm. The range is from 1 to 4294967295.

Defaults Destination address and port address.

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(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 RIB.

This command does not require license.

Examples The following example shows how to set the load-sharing algorithm to use source and destination address:

```
switch(config)# ip load-sharing address source-destination
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

ip load-sharing per-packet

To configure per-packet load sharing on an interface, use the **ip load-sharing per-packet** command. To restore the default, use the **no** form of this command.

ip load-sharing per-packet

no load-sharing per-packet

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines Use the **ip load-sharing per-packet** command to set the load-sharing algorithm on an interface. This command overrides the **ip load-sharing address** command.



Note

Using per-packet load sharing can result in out-of-order packets. Packets for a given pair of source-destination hosts might take different paths and arrive at the destination out of order. Make sure you understand the implications of out-of-order packets to your network and applications. Per-packet load sharing is not appropriate for all networks. Per-flow load sharing ensures packets always arrive in the order that they were sent.

You configure per-packet load sharing on the input interface. This configuration determines the output interface that Cisco NX-OS chooses for the packet.

For example, if you have ECMP paths on two output interfaces, Cisco NX-OS uses the following load-sharing methods for input packets on Ethernet 1/1:

- Per-packet load sharing if you configure configure per-packet load sharing on Ethernet 1/1.
- Per-flow load sharing.

The configuration for the other interfaces have no effect on the load-sharing method used for Ethernet 1/1 in this example.

This command does not require license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to enable per-packet load-sharing on interface Ethernet 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip load-sharing per-packet
```

Related Commands

Command	Description
ip load-sharing	Configures the per-flow load-sharing algorithm.
show ip load-sharing	Displays the load-sharing algorithm.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip name-server

To configure a name server, use the **ip name-server** command. To disable this feature, use the **no** form of the command.

ip name-server *ip-address* [**use-vrf** *name*]

no ip name-server *ip-address* [**use-vrf** *name*]

Syntax Description	ip-address	Specifies the IP address for the name server.
	use-vrf <i>name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to use to reach the name-server. The name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Global configuration VRF context configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ip name-server command to configure the name server for the device. Use the vrf context command to enter the VRF context mode to configure the domain names for a particular VRF. This command does not require a license.

Examples	The following example configures the IP name server for the default VRF. <pre>switch# config terminal switch(config)# ip name-server 192.0.2.1</pre> The following example configures the the IP name server for the management VRF. <pre>switch# config terminal switch(config)# vrf context management switch(config-vrf)# ip name-server 192.0.2.1</pre> The following example configures the the IP name server for the default VRF to use the management VRF as a backup if the the IP name server cannot be reached through the default VRF. <pre>switch# config terminal</pre>

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# ip name-server 192.0.2.1 use-vrf management
```

Related Commands

Command	Description
show hosts	Displays information about the IP domain name configuration.

Send document comments to nexus7k-docfeedback@cisco.com

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 **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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.

Defaults

EIGRP always sets the IP next-hop value to be itself.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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** interface configuration command to instruct EIGRP to use the received next-hop value when advertising these routes.

Examples

The following 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-eigrp-af-if)# no ip next-hop-self eigrp 209
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
prefix-list <i>list-name</i>	Specifies the name of an IP prefix list to filter EIGRP routes.
route-map <i>map-name</i>	Specifies the name of a route map to filter EIGRP routes.
in	Applies route policy to incoming routes.
out	Applies route policy to outgoing routes.
<i>offset</i>	Value to add to the EIGRP metric.

Defaults

This command has no defaults.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip offset-list eigrp** command to influence which route is advertised on an interface. Cisco NX-OS adds the configured offset value to any routes that match the configured prefix list or route map. You must configure the named route map or prefix list to complete this configuration.

This command requires the Enterprise Services license.

Examples

The following 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)# ip offset-list eigrp 209 route-map OffsetFilter in 20
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	prefix-list	Configures a prefix list.
	route-map	Configures a route map.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 <i>key-name</i>	(Optional) Specifies a key chain to use for authentication. The <i>key-name</i> argument can be any alphanumeric string.
message-digest	(Optional) Specifies that message-digest authentication will be used.
null	(Optional) Specifies that no authentication is used. Use the keyword to override any other authentication configured for an area.

Defaults

No authentication

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following example shows how to configure message-digest authentication:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf message-digest-key 33 md5 0 mypassword
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	area authentication	Enables authentication for an OSPF area.
	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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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] *password*

no ip ospf authentication-key

Syntax Description

0	Configures an unencrypted password.
3	Configure a 3DES encrypted password string.
<i>password</i>	Any continuous string of characters that can be entered from the keyboard up to 8 bytes.

Defaults

Unencrypted password

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following example shows how to configure an unencrypted authentication key with the string yourpass:

```
switch(config-if)# ip ospf authentication-key yourpass
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	area authentication	Specifies the authentication type for an OSPF area.
	ip ospf authentication	Specifies the authentication type for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>interface-cost</i>	Unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Defaults

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

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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:

$$\text{link cost} = \text{reference bandwidth} / \text{interface bandwidth}$$

This command requires the Enterprise Services license.

Examples

The following example shows how to configure the interface cost value to 65:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf cost 65
```

Related Commands

Command	Description
reference-bandwidth	Specifies the reference bandwidth that OSPF uses to calculate the link cost.

Send document comments to nexus7k-docfeedback@cisco.com

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

<i>seconds</i>	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. The value must be the same for all nodes on the network.

Defaults

The default for *seconds* is four times the interval set by the **ip ospf hello-interval** command.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip ospf dead-interval** command to set the dead interval that 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 Enterprise Services license.

Examples

The following example shows how to set the OSPF dead interval to 20 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf dead-interval 20
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip ospf hello-interval	Interval between hello packets that OSPF sends on the interface.
show ip ospf interface	Displays OSPF-related information.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>seconds</i> Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.					
Defaults	10 seconds					
Command Modes	Interface configuration					
SupportedUserRoles	network-admin vdc-admin					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(1)	This command was introduced.
Release	Modification					
4.0(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 Enterprise Services license.					
Examples	The following example shows how to set the interval between hello packets to 15 seconds: <pre>switch(config)# interface ethernet 1/2 switch(config-if)# ip ospf hello-interval 15</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip ospf dead-interval</td><td>Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.</td></tr></table>		Command	Description	ip ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.
Command	Description					
ip ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.					

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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**] *key*

no ip ospf message-digest-key *key-id*

Syntax Description

<i>key-id</i>	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.
<i>key</i>	An alphanumeric password of up to 16 bytes.

Defaults

Unencrypted

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following example shows how to set key 19 with the password 8ry4222:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf message-digest-key 19 md5 8ry4222
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication	Specifies the authentication type for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults	OSPF MTU mismatch detection is enabled.

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following example shows how to disable MTU mismatch detection on received DBD packets:

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip ospf mtu-ignore
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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.

Defaults

Depends on the network type.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The network type influences the behavior of the OSPF interface. 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 Enterprise Services license.

Examples

The following example shows how to set an OSPF network as a broadcast network:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.33 255.255.255.0
switch(config-if)# ip ospf network broadcast
```


Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults	Disabled

Command Modes	Interface configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	If an interface is configured as passive-interface it does not participate in the OSPF protocol and will not establish adjacencies or send routing updates. However the interface is announced as part of the routing network.

This command requires the Enterprise Services license.

Examples	The following example shows how to set an interface as passive:

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip ospf passive-interface
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>number-value</i>	Number value that specifies the priority of the router. The range is from 0 to 255.

Defaults

Priority of 1

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 NX-OS uses this priority value when you configure OSPF for broadcast networks using the **neighbor** command in router configuration mode.

This command requires the Enterprise Services license.

Examples

The following example shows how to set the router priority value to 4:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf priority 4
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	ip ospf network	Configures the OSPF network type to a type other than the default for a given medium.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip ospf retransmit-interval

To specify the time between Open Shortest Path First (OSPF) link-state advertisement (LSA) retransmissions for adjacencies belonging 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	<i>seconds</i>	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.

Defaults	5 seconds

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following example shows how to set the retransmit interval value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf retransmit-interval 8
```

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults	None

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ip ospf shutdown command to shut down OSPF on this interface. This command requires the Enterprise Services license.

Examples	The following example shows how to shut down OSPF on an interface: switch(config)# interface ethernet 1/2 switch(config-if)# ip ospf shutdown

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>seconds</i>	Time (in seconds) required to send a link-state update. The range is from 1 to 450 seconds.

Defaults	1 second

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 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 Enterprise Services license.

Examples	The following example shows how to set the transmit delay value to 8 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf transmit-delay 8
```

Send document comments to nexus7k-docfeedback@cisco.com

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 reenble 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

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.

Defaults

Routing updates are sent on the interface.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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)# ip passive-interface eigrp 201
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip policy route-map

To identify a route map to use for policy routing on an interface, use the **ip policy route-map** command. To remove the route map, use the **no** form of this command.

ip policy route-map *name*

no ip policy route-map [*name*]

Syntax Description

<i>name</i>	Name of the route map. The name can be any alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip policy route-map** command to identify a route map to use for policy routing. Use the **route-map** command to create the route map. 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 policy routing is allowed for the interface, based on the destination IP address of the packet. The **set** commands specify the set actions—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip policy route-map** command deletes the pointer to the route map.

You can perform policy-based routing on any match criteria that can be defined in an expanded IP access list when using the **match ip address** command and referencing an expanded IP access list.

You must enable policy-based routing with the **feature pbr** command before you can use the **ip policy route-map** command.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure a policy-based route map to an interface:

```
switch# configure terminal
switch(config)# feature pbr
switch(config)# interface ethernet 2/1
switch(config-if)# ip policy route-map policymap
```

Related Commands

Command	Description
feature pbr	Enabled the policy-based routing feature.
route-map	Creates a route map.
show route-map pbr-statistics	Displays statistics about policy-based route maps

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example enables the generation of ICMP port unreachable messages, as appropriate, on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip port-unreachable
```

Related Commands

Command	Description
ip unreachable	Sends ICMP unreachable messages.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip prefix-list

Use the **ip prefix-list** command to create a prefix list to match IP packets or routes against. 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 prefix-list *name* [**seq** *number*] {**permit** | **deny**} *prefix* [**eq** *length*] [**ge** *length*] [**le** *length*]

Syntax Description	
<i>name</i>	IP prefix list name. The name can be any alphanumeric string up to 63 characters.
seq <i>number</i>	(Optional) Sequence 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.
<i>prefix</i>	IP prefix in A.B.C.D/length format.
eq <i>length</i>	(Optional) Exact prefix length to match. The range is from 1 to 32.
ge <i>length</i>	(Optional) Maximum prefix length to match. The range is from 1 to 32.
le <i>length</i>	(Optional) Minimum prefix length to match. The range is from 1 to 32.

Defaults	None

Command Modes	Global configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

Use the **ip prefix-list** command to configure IP prefix filtering. You 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, providing more flexible configuration than can be configured with just the network/length argument. Cisco NX-OS processes the prefix list using an exact match when you do not configure either neither the **ge** nor **le** keyword. If you configure both the **ge** *ge-length* and **le** *le-length* keywords and arguments, the allowed prefix length range falls between the values used for the ge-length and le-length arguments. The following formula shows this behavior:

network/length < ge *ge-length* < le *le-length* <= 32

Send document comments to nexus7k-docfeedback@cisco.com

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 will be increment by 5 (for example, 5, 10, 15, and onwards). 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 onwards). Default sequence numbers can be suppressed by entering the no form of this command with the seq keyword.

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



Tip

For best performance, the most frequently processed prefix list statements should be configured 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.

This command does not require a license.

Examples

This example shows how to configure a prefix list and apply it to a BGP peer:

```
switch# config t
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
```

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.

Send document comments to nexus7k-docfeedback@cisco.com

ip prefix-list description

Use the **ip prefix-list description** command to configure a description string for an IP prefix-list. 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	<table> <tr> <td><i>name</i></td><td>Name of prefix list. The name can be any alphanumeric string up to 63 characters.</td></tr> <tr> <td><i>string</i></td><td>A descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.</td></tr> </table>	<i>name</i>	Name of prefix list. The name can be any alphanumeric string up to 63 characters.	<i>string</i>	A descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.		
<i>name</i>	Name of prefix list. The name can be any alphanumeric string up to 63 characters.						
<i>string</i>	A descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.						
Defaults	None						
Command Modes	Global configuration						
Supported User Roles	network-admin vdc-admin						
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>4.0(1)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	4.0(1)	This command was introduced.		
Release	Modification						
4.0(1)	This command was introduced.						
Usage Guidelines	This command does not require a license.						
Examples	This example shows how to configure a description for an IP prefix list: <pre>switch# configure terminal switch(config)# ip prefix-list test1 description "this is a test"</pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>ip prefix-list</td><td>Creates an IPv6 prefix list</td></tr> <tr> <td>show ip prefix-list</td><td>Displays information about IPv6 prefix lists.</td></tr> </table>	Command	Description	ip prefix-list	Creates an IPv6 prefix list	show ip prefix-list	Displays information about IPv6 prefix lists.
Command	Description						
ip prefix-list	Creates an IPv6 prefix list						
show ip prefix-list	Displays information about IPv6 prefix lists.						

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable proxy ARPt:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip proxy-arp
```

Send document comments to nexus7k-docfeedback@cisco.com

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 in interface configuration mode. 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	<i>name-of-chain</i> Specifies the group of keys that are valid.				
Defaults	No authentication is provided for RIP packets.				
Command Modes	Interface configuration				
Supported User Roles	network-admin vdc-admin				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
Usage Guidelines	You must separately configure a key chain using the key-chain command to complete the authentication configuration for an interface. This command does not require a license.				
Examples	The following example shows how to configure the interface to accept and send any key that belongs to the key-chain trees: <pre>switch(config)# interface ethernet 1/2 switch(config-if)# ip rip authentication key-chain trees</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>key-chain</td><td>Creates a set of keys that can be used by an authentication method.</td></tr></table>	Command	Description	key-chain	Creates a set of keys that can be used by an authentication method.
Command	Description				
key-chain	Creates a set of keys that can be used by an authentication method.				

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 in interface configuration mode. 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 clear text authentication.
md5	Specifies Message Digest 5 (MD5) authentication.

Defaults

Clear text authentication is provided for RIP packets if you configured a key chain.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

RIPng for IPv6 uses the authentication built into IPv6.

This command does not require a license.

Examples

The following example shows how to configure the interface to use MD5 authentication:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip authentication mode md5
```

Related Commands

Command	Description
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 in interface configuration mode. 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	<i>value</i> Value to add to the incoming route metric for an interface. The range is from 1 to 15. The default is 1.					
Defaults	<i>value</i> : 1					
Command Modes	Interface configuration					
Supported User Roles	network-admin vdc-admin					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(1)	This command was introduced.
Release	Modification					
4.0(1)	This command was introduced.					
Usage Guidelines	Use the ip route metric-offset command to influence which routes are used by Cisco NX-OS. This command allows you to add a fixed offset to the route metric of all incoming routes on an interface. For example, if the you set the metric-offset to 5 on an interface and the incoming route metric is 5, then Cisco NX-OS adds the route to the route table with a metric of 10. This command does not require a license.					
Examples	The following example shows how to configure a metric offset of 10 for all incoming RIP routes on Ethernet interface 2/1: <pre>switch(config)# interface ethernet 2/1 switch(config-if)# ip rip metric-offset 10</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip rip offset-list</td><td>Adds an offset value to incoming RIP route metrics.</td></tr></table>		Command	Description	ip rip offset-list	Adds an offset value to incoming RIP route metrics.
Command	Description					
ip rip offset-list	Adds an offset value to incoming RIP route metrics.					

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 in interface configuration mode. To remove an offset list, use the **no** form of this command.

ip rip offset-list *value*

no ip rip offset-list

Syntax Description

<i>value</i>	Value to add to the incoming route metric for an interface. The range is from 1 to 15. The default is 1.

Defaults

value: 1

Command Modes

Router address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to configure an offset of 10 for all incoming RIP routes on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip rip offset-list 10
```

Related Commands

Command	Description
ip rip metric-offset	Adds an offset value to incoming RIP route metrics.

Send document comments to nexus7k-docfeedback@cisco.com

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 in interface configuration mode. 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.

Defaults	RIP updates are sent on the interface.

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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.

Examples	The following example shows how to configure Ethernet 1/2 as a passive interface:

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip rip passive-interface
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip rip poison-reverse

To enable poison-reverse processing of the Routing Information Protocol (RIP) router updates, use the **ip rip poison-reverse** command in interface configuration mode. 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.

Defaults

Split horizon is always enabled. Poison-reverse processing is disabled.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 NX-OS 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 NX-OS advertises the learned routes as unreachable over the interface on which the route was learned.

This command does not require a license.

Examples

The following example shows how to enable poison-reverse processing for an interface running RIP:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip poison-reverse
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip rip route-filter

To filter the Routing Information Protocol (RIP) routes coming in or out of an interface, use the **route-filter** command in interface configuration mode. 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**}

Syntax Description	prefix-list <i>list-name</i>	Associates a prefix list to filter RIP packets.
	route-map <i>map-name</i>	Associates a route map to set the redistribution policy for RIP.
	in	Filters incoming routes.
	out	Filters outgoing routes.

Defaults	Route filtering is disabled.

Command Modes	Interface configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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.

Examples	The following example shows how to use a route map to filter routes for a RIP interface:

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip rip route-filter route-map InRipFilter in
```

Related Commands	Command	Description
	route-map	Creates a route map.
	prefix-list	Creates a prefix list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip rip summary-address

To configure a summary aggregate address under an interface for the the Routing Information Protocol (RIP), use the **ip rip summary-address** command in interface configuration mode. 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

<i>ip-prefix/length</i>	IP prefix and prefix length to be summarized.

Defaults

Disabled by default.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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.

Examples

The following example shows that the summary address 192.0.2.0 is advertised out Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip summary-address rip 192.0.2.0/24
```

Send document comments to nexus7k-docfeedback@cisco.com

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		
<i>ip-prefix/length</i>		IP prefix and prefix length. The format is x.x.x.x/length. The length is 1 to 32.
<i>interface</i>		(Optional) The interface on which all packets are sent to reach this route. Use ? to display a list of supported interfaces.
<i>next-hop</i>		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.
<i>preference</i>		(Optional) Sets the route preference, used as the administrative distance to this route. The range is from 1 to 255. The default is 1.
tag <i>id</i>		(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.

Defaults	None

Command Modes	Global configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 precedence 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 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, specify an administrative distance greater than 100.

This command does not require a license.

Examples	This example creates 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:

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2
```

This example assigns 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
```

This example chooses a preference of 110. In this case, packets for prefix 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic route information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0/8 172.31.3.4 110
```

Related Commands

Command	Description
ipv6 route	Configures an IPv6 static route.
match tag	matches the tag value associated with a route.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ip router eigrp command to specify the EIGRP instance for the interface. This command requires the Enterprise Services license.

Examples	The following example shows how to set the EIGRP instance for an interface:

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip router eigrp Base
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Instance tag. Specify as an alphanumeric string.
<i>area-id</i>	Identifier for the OSPF area where you want to enable authentication. Specify as either a positive integer value or an IP address.
secondaries none	(Optional) Excludes secondary IP addresses.

Defaults

10 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following example shows how configure an interface for OSPF:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip router ospf Base area 33
```

Send document comments to nexus7k-docfeedback@cisco.com

ip router ospf multi-area

To configure 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	<i>instance-tag</i>	Instance tag. Specify as an case-sensitive alphanumeric string up to 63 characters.
	<i>area-id</i>	Identifier for the OSPF area where you want to add as another area to the primary interface. Specify as either a positive integer value or an IP address.
Defaults	None	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.2(1)	This command was introduced.
Usage Guidelines	Use the ip router ospf multi-area command to specify additional areas on an OSPF interface. This command requires the Enterprise Services license.	
Examples	The following example shows how to configure multi-area adjacency: <pre>switch(config)# interface ethernet 1/2 switch(config-if)# ip router ospf Base area 33 switch(config-if)# ip router ospf Base multi-area 99</pre>	

Send document comments to nexus7k-docfeedback@cisco.com

ip source-route

To handle IP datagrams with source routing header options, use the **ip source-route** command. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route

no ip source-route

Syntax Description

This command has no keywords or arguments.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example enables the handling of IP datagrams with source routing header options: :

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip source-route
```

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>instance-tag</i> Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.	
Defaults	Enabled	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following example shows how to disable split horizon on an Ethernet link: switch(config)# router eigrp 209 switch(config-router)# interface ethernet 2/1 switch(config-eigrp-af-if)# no ip split-horizon eigrp 209	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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*]

no ip summary-address eigrp *instance-tag* {*ip-address /length* | *ip-address mask*}

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>ip-address/length</i>	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 <i>length</i> is used, the slash is required.
<i>ip-address</i>	Summary IP address to apply to an interface in four-part, dotted-decimal notation.
<i>mask</i>	IP address mask.
<i>admin-distance</i>	(Optional) Administrative distance. The range is from 1 to 255.

Defaults

An administrative distance of 5 is applied to EIGRP summary routes.
No summary addresses are predefined.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config-if)# ip summary-address eigrp 209 192.168.0.0/16 95
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip wccp

To enable a Web Cache Communication Protocol (WCCP) service in a service group, use the **ip wccp** command. To disable the service group, use the **no** form of this command.

ip wccp {*service-number* | **web-cache**} [**mode** {**open** [**redirect-list** *access-list*] | **closed** **service-list** *service-access-list*}] [**password** [0-7] *password*]

no ip wccp {*service-number* | **web-cache**} [**mode** {**open** [**redirect-list** *access-list*] | **closed** **service-list** *service-access-list*}] [**password** [0-7] *password*]

Syntax Description

<i>service-number</i>	Dynamic service identifier. The <i>service-number</i> range is from 1 to 255.
web-cache	Specifies the web-cache well-known service.
mode	(Optional) Configures a route tag value for local or direct routes.
open	Identifies the service as open.
closed service-list <i>service-access-list</i>	Identifies the service as closed. The service list identifies a named IP access list that defines the packets that match the service. The <i>service-access-list</i> can be any case-sensitive alphanumeric string up to 64 characters.
redirect-list <i>access-list</i>	(Optional) Specifies the access list that controls traffic redirected to this service group. The <i>access-list</i> can be any case-sensitive alphanumeric string up to 64 characters.
password [0-7]	(Optional) Configures the message digest algorithm 5 (MD5) authentication for messages received from the service group. WCCP discards messages that are not accepted by the authentication. The encryption type can be any value between 0 and 7 (inclusive), where 0 is unencrypted and 7 indicates proprietary encryption.
<i>password</i>	The MD5 password. The <i>password</i> can be any case-sensitive alphanumeric string up to eight characters.

Defaults

None

Command Modes

Global configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

The **redirect-list** keyword instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group. The *access list* specifies the traffic that is permitted to be redirected. The default is to redirect TCP traffic.

Use the **service-list** keyword only for closed mode services. When a WCCP service is closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create a secure connection between the router and the cache engine.

Use **password 0** *pwstring* to store the password in clear text. Use **password 7** *pwstring* to store the password in encrypted form. You can use the **password 7** keywords for an already encrypted password.



Note

You must enter the **ip wccp** command with all your required parameters. Any subsequent entry of the **ip wccp** command overwrites the earlier configuration.

This command does not require a license.

Examples

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
switch(config)# access-list 100
switch(config-acl)# permit ip any any
switch(config-acl)# exit
switch(config)# ip wccp web-cache redirect-list 100
switch(config)# interface ethernet 2/1
switch(config-if)# ip wccp web-cache redirect out
```

The following example shows how to configure a closed WCCP service:

```
switch(config)# ip wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
feature wccp	Enables the WCCP feature.
show ip wccp	Displays the status of the WCCP service group.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip wccp redirect

To redirect a packet on an outbound or inbound interface using the Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command. To disable WCCP redirection, use the **no** form of this command.

ip wccp {*service-number* | **web-cache**} **redirect** {**in** | **out**}

no ip wccp {*service-number* | **web-cache**} **redirect** {**in** | **out**}

Syntax Description

<i>service-number</i>	Dynamic service identifier. The <i>service-number</i> range is from 1 to 255.
web-cache	Specifies the web-cache well-known service.
in	Redirects a packet on an inbound interface.
out	Redirects a packet on an outbound interface.

Defaults

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

WCCPv2 is only supported on Layer 3 interfaces, including Layer 3 subinterfaces, VLAN interfaces, Layer 3 and port channels.

Use the **ip wccp redirect in** command to configure WCCP redirection on an interface that receives inbound network traffic. When you configure the command on an interface, all packets that arrive at that interface are compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they are redirected.

Use the **ip wccp redirect out** command to configure the WCCP redirection check at an outbound interface.

You can also include a redirect list when you configure a service group. The redirect list allows you to deny packets with a NAT (source) IP address and prevent redirection. See the **ip wccp** command for information about configuring the redirect list and service group.

To prevent redirection of any packets from the cache engine, use the **ip wccp redirect exclude in** command on the router interface that faces the cache engine.

Send document comments to nexus7k-docfeedback@cisco.com



Note

Do not use the **ip wccp redirect {in | out}** command and the **ip wccp redirect exclude in** command on the same interface. The **ip wccp redirect exclude in** command overrides the **ip wccp redirect {in | out}** command.

This command does not require a license.

Examples

The following example shows how to configure a session in which WCCP redirects outgoing packets on Ethernet interface 2/2 to a cache engine:

```
switch(config)# ip wccp 99
switch(config)# interface ethernet 2/2
switch(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 2/1 is redirected to a cache engine:

```
switch(config)# ip wccp web-cache
switch(config)# interface ethernet 0/1
switch(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
feature wccp	Enables the WCCP feature.
ip wccp redirect exclude in	Excludes WCCP redirection on an interface.
show ip wccp	Displays the status of the WCCP service group.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ip wccp redirect exclude in

To exclude inbound packets on an interface from Web Cache Communication Protocol (WCCP) redirection checks, use the **ip wccp redirect exclude in** command. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

ip wccp redirect exclude in

no ip wccp redirect exclude in

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **ip wccp redirect exclude in** command to exclude inbound packets on an interface from any redirection check that may occur at the outbound interface. This command affects all the services and should be applied to any inbound interface that will be excluded from redirection.



Note

Do not use the **ip wccp redirect {in | out}** command and the **ip wccp redirect exclude in** command on the same interface. The **ip wccp redirect exclude in** command overrides the **ip wccp redirect {in | out}** command.

This command does not require a license.

Examples

In the following example shows how to exclude packets that arrive on Ethernet interface 2/1 from all WCCP redirection checks:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip wccp redirect exclude in
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
feature wccp	Enables the WCCP feature.
ip wccp redirect	Configures WCCP redirection on an interface.
show ip wccp	Displays the status of the WCCP service group.

Send document comments to nexus7k-docfeedback@cisco.com

ip unreachable

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachable** command. To disable this function, use the no form of this command.

ip unreachable

no ip unreachable

Syntax Description

This command has no keywords or arguments.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example enables the generation of ICMP unreachable messages, as appropriate, on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip unreachable
```

Related Commands

Command	Description
ip port-unreachable	Sends ICMP port unreachable messages.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 address

To configure an IPv6 address on an interface, use the **ipv6 address** command. To remove the address, use the **no** form of this command.

ipv6 address {*addr* [**eui64**] [**route-preference** *preference*] [**secondary**] **tag** *tag-id*] | **use-link-local-only**}

no ipv6 address {*addr* [**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*] | **use-link-local-only**}

Syntax Description	<i>addr</i>	IPv6 address. The format is A:B::C:D/length. The length range is 1 to 128.
	eui64	(Optional) Configures the Extended Unique Identifier (EUI64) for the low-order 64 bits of the address.
	route-preference <i>preference</i>	(Optional) Sets the route preference for local or direct routes. The range is from 0 to 255.
	secondary	(Optional) Creates a secondary IPv6 address.
	tag <i>tag-id</i>	(Optional) Configures a route tag value for local or direct routes.

Defaults	None

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	Added tag keyword.

Usage Guidelines	Use the ipv6 address command to configure an IPv6 address or secondary address on an interface. This command does not require a license.

Examples	This example shows how to configure an IPv6 address: <pre>switch# conf t switch(config)# interface ethernet 2/1 switch(config-if)# ipv6 address 2001:0DB8::3/48</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip address	Configures an IPv4 address on an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 authentication key-chain eigrp

To enable authentication for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets and to specify the set of keys that can be used on an interface, use the **ipv6 authentication key-chain eigrp** command. To prevent authentication, use the **no** form of this command.

ipv6 authentication key-chain eigrp *instance-tag name-of-chain*

no ipv6 authentication key-chain eigrp *instance-tag name-of-chain*

Syntax Description	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	<i>name-of-chain</i>	Name of a key chain. The key chain name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults No authentication is provided for EIGRP packets.

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines You must set the authentication mode using the **ipv6 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 Enterprise Services license.

Examples The following 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)# ipv6 authentication key-chain eigrp 209 trees
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ipv6 authentication mode eigrp	Sets the authentication mode for EIGRP for an IPv6 interface.
key-chain	Creates a set of keys that can be used by an authentication method.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 authentication mode eigrp

To specify the type of authentication used in the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **ipv6 authentication mode eigrp** command. To remove authentication, use the **no** form of this command.

ipv6 authentication mode eigrp *instance-tag* **md5**

no ipv6 authentication mode eigrp *instance-tag* **md5**

Syntax Description	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	md5	Specifies Message Digest 5 (MD5) authentication.

Defaults	None

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following 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)# ipv6 authentication mode eigrp 209 md5
```

Related Commands	Command	Description
	authentication mode (EIGRP)	Configures the authentication mode for EIGRP in address-family mode.
	iv6p 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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 bandwidth eigrp

To configure the bandwidth metric on an Enhanced Interior Gateway Routing Protocol (EIGRP) for the IPv6 interface, use the **ipv6 bandwidth eigrp** command. To restore the default, use the **no** form of this command.

ipv6 bandwidth eigrp *instance-tag* *bandwidth*

no ipv6 bandwidth eigrp

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>bandwidth</i>	Bandwidth value. The range is from 1 to 2,560,000,000 kilobits.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following 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)# ipv6 bandwidth eigrp 209 10000
```

Related Commands

Command	Description
ipv6 bandwidth-percent eigrp	Sets the percent of the interface bandwidth that EIGRP can use.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 bandwidth-percent eigrp** command. To restore the default, use the **no** form of this command.

ipv6 bandwidth-percent eigrp *instance-tag percent*

no ipv6 bandwidth-percent eigrp

Syntax Description	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	<i>percent</i>	Percentage of bandwidth that EIGRP may use.

Defaults	<i>percent</i> : 50

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	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 Enterprise Services license.

Examples	The following 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)# ipv6 bandwidth-percent eigrp 209 75
```

Related Commands	Command	Description
	ipv6 bandwidth eigrp	Sets the EIGRP bandwidth value for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 delay eigrp

To configure the throughput delay for the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 delay eigrp** command. To restore the default, use the **no** form of this command.

ipv6 delay eigrp *instance-tag seconds*

no ipv6 delay eigrp *instance-tag*

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>seconds</i>	Throughput delay, in tens of microseconds. The range is from 1 to 16777215.

Defaults

100 (10-microsecond units)

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You configure the throughput delay on an interface in 10-microsecond units. For example, if you set the **ipv6 delay eigrp** command to 100, the throughput delay is 1000 microseconds.

This command requires the Enterprise Services license.

Examples

The following 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)# ipv6 delay eigrp 1 40
```

Related Commands

Command	Description
ipv6 hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process that is designated by an autonomous system number.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 distribute-list eigrp

To configure a distribution list for the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 distribute-list eigrp** command. To restore the default, use the **no** form of this command.

ipv6 distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

no ipv6 distribute-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

Syntax Description	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	prefix-list <i>list-name</i>	Specifies the name of an IPv6 prefix list to filter EIGRP routes.
	route-map <i>map-name</i>	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.

Defaults	None

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	Use the ipv6 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 Enterprise Services license.

Examples	The following example shows how to configure a route map for all EIGRP routes coming into the interface: <pre>switch(config)# router eigrp 209 switch(config-router)# interface ethernet 2/1 switch(config-if)# ipv6 distribute-list eigrp 209 route-map InputFilter in</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 eigrp shutdown

To shut down the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 eigrp shutdown** command. To restore the default, use the **no** form of this command.

ipv6 eigrp *instance-tag* **shutdown**

no ipv6 eigrp *instance-tag* **shutdown**

Syntax Description	<i>instance-tag</i> Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.	
Defaults	None	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.1(2)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Examples	The following example shows how to disable EIGRP on an interface: switch(config)# router eigrp 201 switch(config-router)# interface ethernet 2/1 switch(config-if)# ipv6 eigrp 201 shutdown	
Related Commands	Command	Description
	router eigrp	Configures an instance of EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 hello-interval eigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 hello interval for an interface, use the **ipv6 hello-interval eigrp** command. To restore the default, use the **no** form of this command.

ipv6 hello-interval eigrp *instance-tag* *seconds*

no ipv6 hello-interval eigrp *instance-tag*

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>seconds</i>	Hello interval (in seconds). The range is from 1 to 65535.

Defaults

5 seconds

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following 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)# ipv6 hello-interval eigrp 1 10
```

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 hold-time eigrp

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 interface, use the **ipv6 hold-time eigrp** command. To restore the default, use the **no** form of this command.

ipv6 hold-time eigrp *instance-tag seconds*

no ipv6 hold-time eigrp *instance-tag*

Syntax Description	<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
	<i>seconds</i>	Hold time (in seconds). The range is from 1 to 65535.

Defaults	15 seconds

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	Use the ipv6 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 Enterprise Services license.

Examples	The following example shows how to set the hold time to 40 seconds for the interface:
	<pre>switch(config)# router eigrp 209</pre>
	<pre>switch(config-router)# interface ethernet 2/1</pre>
	<pre>switch(config-if)# ipv6 hold-time eigrp 209 40</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ipv6 hello-interval eigrp	Configures the hello interval on an interface for the EIGRP routing process designated by an autonomous system number.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache, use the **ipv6 host** command. To remove a hostname-to-address mapping, use the **no** form of this command.

ipv6 host *name address1* [*address2... address6*]

no ipv6 host *name address1* [*address2... address6*]

Syntax Description	<i>name</i>	Hostname. The <i>name</i> can be any case-sensitive alphanumeric string up to 80 characters.
	<i>address1</i>	IPv6 address in the A:B::C:D format.
	<i>address2 ...address6</i>	(Optional) Up to five additional IPv6 addresses in the A:B::C:D format.
Defaults	None	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.1(2)	This command was introduced.
Usage Guidelines	Use the ipv6 host command to add a static hostname to DNS. This command does not require a license.	
Examples	The following example shows how to configure a static hostname: switch(config)# ipv6 host mycompany.com 2001:0DB8::4	
Related Commands	Command	Description
	ip host	Configures a static hostname.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 nd hop-limit

To advertise the hop limit in IPv6 neighbor discovery packets, use the **ipv6 nd hop-limit** command. To return to default, use the **no** form of this command.

ipv6 nd hop-limit *hop-limit*

no ipv6 nd hop-limit [*hop-limit*]

Syntax Description

<i>hop-limit</i>	Hop limit in IPv6 header. The range is from 0 to 255.

Defaults

64

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the IPv6 hop limit:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd hop-limit 55
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd managed-config-flag

To advertise in ICMPv6 Router-Advertisement messages to use stateful address auto-configuration to obtain address information, use the **ipv6 nd managed-config-flag** command. To revert to default, use the **no** form of this command.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows how to advertise in ICMPv6 Router-Advertisement messages to use stateful address auto-configuration to obtain address information:

```
switch(config)# interface ethernet 2/1  
switch(config-if)# ipv6 nd managed-config-flag
```

Related Commands	Command	Description
	show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd mtu

To advertise the MTU in ICMPv6 Router-Advertisement messages on this link, use the **ipv6 nd mtu** command. To revert to default, use the **no** form of this command.

ipv6 nd mtu *mtu*

no ipv6 nd mtu [*mtu*]

Syntax Description

<i>mtu</i>	MTU in bytes. The range is from 1280 to 65535.

Defaults

1500

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the MTU value to advertise on a link:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd mtu 1280
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd ns-interval

To configure the retransmission interval between IPv6 neighbor solicitation messages, use the **ipv6 nd ns-interval** command. To revert to default, use the **no** form of this command.

ipv6nd ns-interval *interval*

no ipv6 nd ns-interval [*interval*]

Syntax Description	<i>interval</i> Interval in milliseconds. The range is from 1000 to 3600000.				
Defaults	1000				
Command Modes	Interface configuration				
Supported User Roles	network-admin vdc-admin				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
Usage Guidelines	This command does not require a license.				
Examples	This example shows how to configure the neighbor solicitation interval: <pre>switch(config)# interface ethernet 2/1 switch(config-if)# ipv6 nd ns-interval 1280</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ipv6 nd interface</td><td>Displays IPv6 neighbor discovery information for an interface.</td></tr></table>	Command	Description	show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.
Command	Description				
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.				

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd other-config-flag

To indicate in ICMPv6 router advertisement messages that hosts use stateful auto-configuration to obtain non-address related information, use the **ipv6 nd other-config-flag** command. To revert to default, use the **no** form of this command.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure stateful autoconfiguration in ICMPv6 router advertisement messages:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 nd ra-interval

To configure the interval between sending ICMPv6 router advertisement messages, use the **ipv6 nd ra-interval** command. To revert to default, use the **no** form of this command.

ipv6 nd ra-interval *interval*

no ipv6 nd ra-interval [*interval*]

Syntax Description	<i>interval</i> Interval between sending router advertisement messages in seconds. The range is from 4 to 1800.	
Defaults	600	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the ICMPv6 router advertisement message interval: switch(config)# interface ethernet 2/1 switch(config-if)# ipv6 nd ra-interval 500	
Related Commands	Command	Description
	show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 nd ra-lifetime

To advertise the router lifetime of a default router in ICMPv6 router advertisement messages, use the **ipv6 nd ra-lifetime** command. To revert to default use the **no** form of this command.

ipv6 nd ra-lifetime *lifetime*

no ipv6 nd ra-lifetime [*lifetime*]

Syntax	Description
<i>lifetime</i>	Lifetime in seconds. The range is from 0 to 9000. If 0, this router will not be the default router.

Defaults	Three times the router advertisement interval.

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows how to configure the ICMPv6 router advertisement message lifetime:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd ra-lifetime 1500
```

Related Commands	Command	Description
	show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd reachable-time

To advertise the time when a node considers a neighbor up after receiving a reachability confirmation in ICMPv6 router advertisement messages, use the **ipv6 nd reachable-time** command. To revert to default, use the **no** form of this command.

ipv6 nd reachable-time *time*

no ipv6 nd reachable-time [*time*]

Syntax	Description	
	<i>time</i>	Time in milliseconds. The range is from 0 to 3600000.
Defaults	0	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the ICMPv6 router advertisement reachability time: switch(config)# interface ethernet 2/1 switch(config-if)# ipv6 nd reachable-time 1500	
Related Commands	Command	Description
	show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd redirects

To enable sending ICMPv6 redirect messages, use the **ipv6 redirects** command. To revert to default, use the **no** form of this command.

ipv6 nd redirects

no ipv6 nd redirects

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to disable the ICMPv6 router advertisement messages:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd retrans-timer

To advertise the time between neighbor solicitation (NS) messages in ICMPv6 router advertisement messages, use the **ipv6 nd retrans-timer** command. To revert to default, use the **no** form of this command.

ipv6 nd retrans-timer *time*

no ipv6 nd retrans-timer [*time*]

Syntax	Description	
	<i>time</i>	Time in milliseconds. The range is from 0 to 4294967295.
Defaults	0	
Command Modes	if-igmp configuration (config-xxx)	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the ICMPv6 router advertisement reachability time: <pre>switch(config)# interface ethernet 2/1 switch(config-if)# ipv6 nd reachable-time 1500</pre>	
Related Commands	Command	Description
	show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 nd suppress-ra

To disable sending ICMPv6 router advertisement messages, use the **ipv6 nd suppress-ra** command. To revert to default, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description

This command has no keywords or arguments.

Defaults

Enabled

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to disable the ICMPv6 router advertisement messages:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *pv6-address interface-type interface-number hardware-address*

no ipv6 neighbor *ipv6-address interface-type interface-number hardware-address*

Syntax Description	<i>ipv6-address</i>	The IPv6 address that corresponds to the local data-link address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
	<i>interface-type</i>	The specified interface type. For supported interface types, use the question mark (?) online help function.
	<i>interface-number</i>	The specified interface number.
	<i>hardware-address</i>	The local data-link address (a 48-bit address).

Defaults	None

Command Modes	Interface configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ipv6 neighbor command to create a static entry. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.
	Use the show ipv6 neighbors command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states: • INCMP (Incomplete)—The interface for this entry is down. • REACH (Reachable)—The interface for this entry is up.

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries. See the `show ipv6 neighbors` command for descriptions of the INCMP and REACH states for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache, except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command or the **no ipv6 unnumbered** command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to INCMP).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Examples

The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 neighbor 2001:0DB8::45A ethernet 2/10002.7D1A.9472
```

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 next-hop-self eigrp

To instruct the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 process to use the local IPv6 address as the next-hop address when advertising these routes, use the **next-hop-self eigrp** command. To use the received next-hop value, use the **no** form of this command.

ipv6 next-hop-self eigrp *instance-tag*

no ipv6 next-hop-self eigrp *instance-tag*

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.

Defaults

EIGRP always sets the IPv6 next-hop value to be itself.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

EIGRP, by default, sets the IPv6 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 ipv6 next-hop-self eigrp** interface configuration command to instruct EIGRP to use the received next-hop value when advertising these routes.

Examples

The following example shows how to change the default IPv6 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-eigrp-af-ipv6)# no ipv6 next-hop-self eigrp 209
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 offset-list eigrp

To configure an offset list for the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 offset-list eigrp** command. To restore the default, use the **no** form of this command.

ipv6 offset-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

no ipv6 offset-list eigrp *instance-tag* {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**} *offset*

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
prefix-list <i>list-name</i>	Specifies the name of an IPv6 prefix list to filter EIGRP routes.
route-map <i>map-name</i>	Specifies the name of a route map to filter EIGRP routes.
in	Applies a route policy to incoming routes.
out	Applies a route policy to outgoing routes.
<i>offset</i>	Value to add to the EIGRP metric.

Defaults

This command has no defaults.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 offset-list eigrp** command to influence which route is advertised on an interface. Cisco NX-OS adds the configured offset value to any routes that match the configured prefix list or route map. You must configure the named route map or prefix list to complete this configuration.

This command requires the Enterprise Services license.

Examples

The following 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)# ipv6 offset-list eigrp 209 route-map OffsetFilter in 20
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
prefix-list	Configures a prefix list.
route-map	Configures a route map.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 passive-interface eigrp

To suppress all routing updates on an Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 interface, use the **ipv6 passive-interface eigrp** command. To reenale the sending of routing updates, use the **no** form of this command.

ipv6 passive-interface eigrp *instance-tag*

no ipv6 passive-interface eigrp *instance-tag*

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.

Defaults

Routing updates are sent on the interface.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 passive-interface eigrp** command to stop all routing updates on an interface and suppress the formation of EIGRP adjacencies.

This command requires the Enterprise Services license.

Examples

The following 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)# ipv6 passive-interface eigrp 201
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 policy route-map

To identify a route map to use for policy routing on an interface, use the **ipv6 policy route-map** command. To remove the route map, use the **no** form of this command.

ipv6 policy route-map *name*

no ipv6 policy route-map [*name*]

Syntax Description	<i>name</i> Name of the route map. The name can be any alphanumeric string up to 63 characters.	
Defaults	None	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.2(1)	This command was introduced.
Usage Guidelines	Use the iv6 policy route-map command to identify a route map to use for policy routing on an IPv6 interface. Use the route-map command to create the rout map. 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 policy routing is allowed for the interface, based on the destination IPv6 address of the packet. The set commands specify the set actions—the particular policy routing actions to perform if the criteria enforced by the match commands are met. The no ipv6 policy route-map command deletes the pointer to the route map. You can perform policy-based routing on any match criteria that can be defined in an IPv6 access list when using the match ipv6 address command and referencing an IPv6 access list. You must enable policy-based routing with the feature pbr command before you can use the ipv6 policy route-map command. This command requires the Enterprise Services license.	

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure a policy-based route map to an interface:

```
switch# configure terminal
switch(config)# feature pbr
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 policy route-map policymap
```

Related Commands

Command	Description
feature pbr	Enabled the policy-based routing feature.
route-map	Creates a route map.
show route-map pbr-statistics	Displays statistics about policy-based route maps
show ipv6 policy	Displays information about IPv6 policies

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 prefix-list

Use the **ipv6 prefix-list** command to create a prefix list to match IPv6 packets or routes against. To remove the prefix-list, use the **no** form of this command.

ipv6 prefix-list *name* [**seq number**] {**permit** | **deny**} *prefix* [**eq length** | [**ge length**] [**le length**]]

no ipv6 prefix-list *name* [**seq number**] {**permit** | **deny**} *prefix* [**eq length** | [**ge length**] [**le length**]]

Syntax Description	
<i>name</i>	IPv6 prefix list name. The name can be any alphanumeric string up to 63 characters.
<i>seq number</i>	(Optional) Sequence 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.
<i>prefix</i>	IP prefix in A:B::C:D/length format.
<i>eq length</i>	(Optional) Exact prefix length to match. The range is from 1 to 128.
<i>ge length</i>	(Optional) Maximum prefix length to match. The range is from 1 to 128.
<i>le length</i>	(Optional) Minimum prefix length to match. The range is from 1 to 128.

Defaults None

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **ipv6 prefix-list** command to configure IPv6 prefix filtering. You 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 IPv6 address and a bit mask. The bit mask is entered as a number from 1 to 128. 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, providing more flexible configuration than can be configured with just the network/length argument. Cisco NX-OS processes the prefix list using an exact match when you do not configure either neither the **ge** nor **le** keyword. If you configure both the **ge ge-length** and **le le-length** keywords and arguments, the allowed prefix length range falls between the values used for the ge-length and le-length arguments. The following formula shows this behavior:

Send document comments to nexus7k-docfeedback@cisco.com

network/length < ge ge-length < le le-length <= 32

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 will be increment by 5 (for example, 5, 10, 15, and onwards). 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 onwards). Default sequence numbers can be suppressed by entering the no form of this command with the seq keyword.

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



Tip

For best performance, the most frequently processed prefix list statements should be configured 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 ipv6 prefix-list** command. Prefix-list counters can be reset by entering the **clear ipv6 prefix-list** command.

This command does not require a license.

Examples

This example shows how to configure an IPv6 prefix list and apply it to a BGP peer:

```
switch# config t
switch(config)# ipv6 prefix-list allowprefix 10 permit 2001:0DB8::/48 eq 24
switch(config) router bgp 65536:20
switch(config-router)# neighbor 2001:0DB8::1/64 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv6 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
```

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.

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 prefix-list description

Use the **ipv6 prefix-list description** command to configure a description string for an IPv6 prefix-list. To revert to default, use the **no** form of this command.

ipv6 prefix-list *name* **description** *string*

no ipv6 prefix-list *name* **description**

Syntax Description	<i>name</i>	Name of prefix list. The name can be any alphanumeric string up to 63 characters.
	<i>string</i>	A descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.
Defaults	None	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure a description for an IPv6 prefix list:	
	<pre>switch# configure terminal switch(config)# ipv6 prefix-list test1 description "this is a test"</pre>	
Related Commands	Command	Description
	ipv6 prefix-list	Creates an IPv6 prefix list
	show ipv6 prefix-list	Displays information about IPv6 prefix lists.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 route

To configure a static IPv6 route, use the **ipv6 route command** command. To remove this static route, use the **no** form of this command.

ipv6 route *ipv6-prefix/length* { {*next-hop-addr* | *next-hop-prefix*} | *interface* | *link-local-addr*} [*preference*] [**tag** *tag-id*]

no ipv6 route *ipv6-prefix/length*

Syntax Description

<i>ipv6-prefix/length</i>	IPv6 prefix and prefix length. The format is A:B::C:D/length. The length range is from 1 to 128.
<i>next-hop</i>	The next-hop address. The format is A:B::C:D.
<i>next-hop-prefix</i>	The next-hop prefix and length. The format is A:B::C:D/length. The length range is from 1 to 128.
<i>interface</i>	The interface to reach this route. Use ? to display a list of supported interfaces.
<i>link-local-addr</i>	The IPv6 link-local address. The format is A:B::C:D.
<i>preference</i>	(Optional) Sets the route preference, used as the administrative distance to this route. The range is from 1 to 255. The default is 1.
tag <i>id</i>	(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.

Defaults

Disabled by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example creates an IPv6 static route:

```
switch(config)# ipv6 route 2001:0DB8::/48 2b11::2f01:4c
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip route	Configures an IPv4 static route.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 router eigrp

To specify the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 interface, use the **ipv6 router eigrp** command. To return to the default, use the **no** form of this command.

ipv6 router eigrp *instance-tag*

no ipv6 router eigrp *instance-tag*

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 router eigrp** command to specify the EIGRP instance for the interface. This command requires the Enterprise Services license.

Examples

The following example shows how to set the EIGRP instance for an interface:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router eigrp Base
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 router ospfv3 area

To specify the Open Shortest Path First version 3(OSPFv3) instance and area for an interface, use the **ipv6 router ospfv3 area** command. To return to the default, use the **no** form of this command.

ipv6 router ospfv3 *instance-tag* **area** *area-id* [**secondaries none**]

no ipv6 router ospfv3 *instance-tag* **area** *area-id* [**secondaries none**]

Syntax Description	<i>instance-tag</i>	Instance tag. Specify as an alphanumeric string.
	<i>area-id</i>	Identifier for the OSPFv3 area where you want to enable authentication. Specify as either a positive integer value or an IP address.
	secondaries none	(Optional) Excludes secondary IP addresses.
Defaults	None	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Use the ipv6 router ospfv3f area command to specify the area and OSPFv3 instance for the interface. This command requires the Enterprise Services license.	
Examples	The following example shows how configure an interface for OSPFv3:	
	<pre>switch(config)# interface ethernet 1/2 switch(config-if)# ipv6 router ospfv3 Base area 33</pre>	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 router ospfv3 multi-area

To configure multi-area adjacency on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 router ospfv3 multi-area** command. To return to the default, use the **no** form of this command.

```
ipv6 router ospfv3 instance-tag multi-area area-id

no ipv6 router ospfv3 instance-tag multi-area area-id
```

Syntax Description	instance-tag	Instance tag. Specify as an case-sensative alphanumeric string up to 63 characters.
	area-id	Identifier for the OSPF area where you want to add as another area to the primary interface. Specify as either a positive integer value or an IP address.

DefaultsNone

Command ModesInterface configuration

SupportedUserRolesnetwork-admin
vdc-admin

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage GuidelinesUse the **ipv6 router ospfv3 multi-area** command to specify aditional areas on an OSPFv3 interface. This command requires the Enterprise Services license.

ExamplesThe following example shows how to configure multi-area adjacency:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router ospfv3 Base area 33
switch(config-if)# ipv6 router ospfv3 Base multi-area 99
```


Send document comments to nexus7k-docfeedback@cisco.com

ipv6 split-horizon eigrp

To enable split horizon for an Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 process, use the **ipv6 split-horizon eigrp** command. To disable split horizon, use the **no** form of this command.

ipv6 split-horizon eigrp *instance-tag*

no ipv6 split-horizon eigrp *instance-tag*

Syntax Description	<i>instance-tag</i> Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.	
Defaults	Enabled	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.1(2)	This command was introduced.
Usage Guidelines	Use the no ipv6 split-horizon eigrp command to disable split horizon on an interface. This command requires the Enterprise Services license.	
Examples	The following example shows how to disable split horizon on an Ethernet link: switch(config)# router eigrp 209 switch(config-router)# interface ethernet 2/1 switch(config-eigrp-af-if)# no ipv6 split-horizon eigrp 209	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ipv6 summary-address eigrp

To configure a summary aggregate address for the specified Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 interface, use the **ipv6 summary-address eigrp** command. To disable a configuration, use the **no** form of this command.

ipv6 summary-address eigrp *instance-tag* {*ipv6-address /length*} [*admin-distance*]

no ipv6 summary-address eigrp *instance-tag* {*ipv6-address /length*}

Syntax Description

<i>instance-tag</i>	Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.
<i>ipv6-address/length</i>	Summary IPv6 prefix and prefix length to apply to an interface in A:B::C:D/length format. The length range is from 1 to 128.
<i>admin-distance</i>	(Optional) Administrative distance. The range is from 1 to 255.

Defaults

An administrative distance of 5 is applied to EIGRP summary routes.
No summary addresses are predefined.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **ipv6 summary-address eigrp** command to configure interface-level summary address. EIGRP summary routes are given an administrative distance of 5.

This command requires the Enterprise Services license.

Examples

The following example shows how to configure an administrative distance of 95 on an EIGRP interface for the 2001:0DB8::/48 summary address:

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 summary-address eigrp 209 2001:0DB8::/48 95
```

Send document comments to nexus7k-docfeedback@cisco.com

ipv6 unreachable

To enable sending ICMPv6 unreachable messages, use the **ipv6 unreachable** command. To revert to default, use the **no** form of this command.

ipv6 [icmp] unreachable

no ipv6 [icmp] unreachable

Syntax	Description	
	icmp	(Optional) ICMPv6 commands.
Defaults	Disabled	
Command Modes	Interface configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Port-unreachable messages are always rate-limit enabled. This command does not require a license.	
Examples	This example shows how to enable the ICMPv6 unreachable messages: switch(config)# interface ethernet 2/1 switch(config-if)# ipv6 unreachable	
Related Commands	Command	Description
	show ipv6 nd interface	Displays IPv6 neighbor discovery information for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

is-type

To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the **is-type** command. To reset the default value, use the **no** form of this command.

is-type {level-1 | level-1-2 | level-2}

no is-type {level-1 | level-1-2 | level-2}

Syntax Description

level-1	Specifies that the router performs only level-1 (intraarea) routing.
level-1-2	Specifies that the router performs both level-1 and level-2 routing.
level-2	Specifies that the routing process acts as a level-2 (interarea) router only.

Command Default

Routers typically act as both a level-1 (intraarea) and a level-2 (interarea) router by default. In multiarea IS-IS configurations, the first instance of the IS-IS routing process configured is by default a level-1-2 (intraarea and interarea) router. The remaining instances of the IS-IS process configured by default are level-1 routers.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The routing levels for an instance of the IS-IS routing process are defined as follows:

- **level-1**—Specifies that the router performs only level-1 (intraarea) routing. This router learns only about destinations inside its area. Level-2 (interarea) routing is performed by the closest level-1-2 router.
- **level-1-2**—Specifies that the router performs both level-1 and level-2 routing. This router runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (level-1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (level-2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.
- **level-2**—Specifies that the routing process acts as a level-2 (interarea) router only. This router is part of the backbone, and does not communicate with level-1-only routers in its own area.

Send document comments to nexus7k-docfeedback@cisco.com

We recommend that you configure the type of IS-IS routing process. If you are configuring multiarea IS-IS, you must configure the type of the router, or allow it to be configured by default. By default, the first instance of the IS-IS routing process that you configure using the `router isis` command is a level-1-2 router.

If only one area is in the network, there is no need to run both level-1 and level-2 routing algorithms. If IS-IS is used for IP routing only (and there is only one area), you can run level-2 only everywhere. Areas you add after the level-1-2 area exists are by default level-1 areas.

If the router instance has been configured for level-1-2 (the default for the first instance of the IS-IS routing process in a Cisco device), you can remove level-2 (interarea) routing for the area using the `is-type` command. You can also use the `is-type` command to configure level-2 routing for an area, but it must be the only instance of the IS-IS routing process configured for level-2 on the Cisco device.

This command requires the Enterprise Services license.

Examples

The following example specifies an area router:

```
switch(config)# router isis  
switch(config-router)# is-type level-2-only
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

isis authentication key-chain

To enable authentication for Intermediate System-to-Intermediate System (IS-IS) for an individual IS-IS interface, use the **isis authentication key-chain** *auth-key* {**level-1** | **level-2**} command. To disable such authentication, use the **no** form of this command.

isis authentication key-chain *auth-key* {**level-1** | **level-2**}

no isis authentication key-chain *auth-key* {**level-1** | **level-2**}

Syntax Description

<i>auth-key</i>	Authentication key chain.
level-1	Specifies the authentication key for level-1 link state packets (LSP), complete sequence number packets (CSNP), and partial sequence number packets (PSNP) only.
level-2	Specifies the authentication key for level-2 LSP, CSNP and PSNP packets only.

Command Default

No key chain authentication is provided for IS-IS packets at the router level.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If no key chain is configured with the **isis authentication key-chain** command, no key chain authentication is performed.

Key chain authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the authentication mode command.

Only one authentication key chain is applied to IS-IS at one time. For example, if you configure a second **isis authentication key-chain** command, the first authentication key chain is overridden.

You can configure key-chain authentication per IS-IS instance by using the **authentication key-chain** configuration command.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com**Examples**

The following example configures IS-IS to accept and send any key belonging to the key chain named site1 on a specific interface:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication key-chain site1 level-1
switch(config-if)#
```

Related Commands

Command	Description
authentication key-chain	Enables authentication per IS-IS instance.
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

isis authentication-check

To specify for the Intermediate System-to-Intermediate System (IS-IS) instance that authentication is performed only on IS-IS packets being sent (not received) from an interface, use the **isis authentication-check** command. To configure for the IS-IS instance that if authentication is configured at the router level, such authentication be performed on packets being sent and received, use the **no** form of this command.

authentication-check { level-1 | level-2 }

no authentication-check

Syntax Description

level-1	Specifies that authentication is performed only on level-1 packets that are being sent (not received)
level-2	Specifies that authentication is performed only on level-2 packets that are being sent (not received).

Command Default

If authentication is configured at the router level, it applies to IS-IS packets being sent and received.

Command Modes

Interface configuration

Usage Guidelines

Enter the **isis authentication-check** command before configuring the authentication mode and authentication key chain. Entering the **isis authentication-check** command allows the routers to have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After you enter the authentication-check command on all communicating routers, enable the authentication mode and key chain on each router. Then enter the **no isis authentication-check** command to disable the command.

This command could apply to clear text authentication or Message Digest 5 (MD5) authentication. The mode is determined by the authentication mode command.

You can specify authentication check per IS-IS instance by using the **authentication-check** configuration mode command.

This command requires the Enterprise Services license.

Examples

The following example configures IS-IS level-1 packets on a specific interface to use clear text authentication on packets being sent (not received):

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication-check level-1
switch(config-if)# isis authentication key-chain site1 level-1
switch(config-if)#
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	authentication-check	Specifies that authentication is performed only on IS-IS packets being sent (not received).
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

isis authentication-type

To specify the type of authentication used in Intermediate System-to-Intermediate System (IS-IS) packets on a specific interface, use the **isis authentication-type** command. To restore clear text authentication, use the **no** form of this command.

isis authentication-type { **cleartext** | **md5** } [**level-1** | **level-2**]

no isis authentication-type

Syntax Description

cleartext	Specifies clear text authentication.
md5	Specifies Message Digest 5 (MD5) authentication.
level-1	Enables the specified authentication for level-1 link state packet (LSP), complete sequence number packet (CSNP) and partial sequence number packet (PSNP) packets only.
level-2	Enables the specified authentication for level-2 LSP, CSNP and PSNP packets only.

Command Default

No authentication is provided for IS-IS packets at the router level by use of this command.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If you do not enter the **level-1** or **level-2** keywords, the mode applies to both levels.

You can specify the authentication type per IS-IS instance by using the **authentication-type** configuration mode command.

This command requires the Enterprise Services license.

Examples

The following example configures for the IS-IS instance that Message Digest 5 (MD5) authentication is performed on level-1 packets on a specific interface:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication-type md5 level-1
switch(config-router)#
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	authentication-type	Specifies the authentication type per IS-IS instance.
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

isis circuit-type

To configure the type of adjacency, use the **isis circuit-type** command. To reset the circuit type to Level 1 and Level 2, use the **no** form of this command.

isis circuit-type { **level-1** | **level-1-2** | **level-2-only** }

no isis circuit-type

Syntax Description

level-1	Configures a router for Level 1 adjacency only.
level-1-2	Configures a router for Level 1 and Level 2 adjacency.
level-2-only	Configures a router for Level 2 adjacency only.

Command Default

A Level 1 and Level 2 adjacency is established.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You do not have to configure this command. We recommend that you configure a router as a Level 1-only, Level 1-2, or Level 2-only system. Only on routers that are between areas (Level 1-2 routers) should you configure some interfaces to be Level 2-only to prevent wasting bandwidth by sending out unused Level 1 hello packets. Note that on point-to-point interfaces, the Level 1 and Level 2 hellos are in the same packet.

A Level 1 adjacency may be established if there is at least one area address in common between this system and its neighbors. Level 2 adjacencies will never be established over this interface.

A Level 1 and Level 2 adjacency is established if the neighbor is also configured as level-1-2 and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.

Level 2 adjacencies are established if the other routers are Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies will never be established over this interface.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

In the following example, other routers on Ethernet interface 2/5 are in the same area. Other routers on Ethernet interface 1 are in other areas, so the router will stop sending Level 1 hellos.

```
switch(config)# router isis test1  
switch(config-router)# interface ethernet 2/5  
switch(config-if)# isis circuit-type level-2-only  
switch(config-if)#
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

isis csnp-interval

To configure the Intermediate System-to-Intermediate System (IS-IS) complete sequence number (CSNPs) interval, use the **isis csnp-interval** command. To restore the default value, use the **no** form of this command.

isis csnp-interval *seconds* {**level-1** | **level-2**}

no isis csnp-interval [**level-1** | **level-2**]

Syntax Description

<i>seconds</i>	Interval of time (in seconds) between transmission of CSNPs on multiaccess networks. This interval only applies for the designated router. Range: 0 to 65535. Default: 10.
level-1	Configures the interval of time between transmission of CSNPs for Level 1 independently.
level-2	Configures the interval of time between transmission of CSNPs for Level 2 independently.

Command Default

The default settings are as follows:

- 10 seconds
- Level 1 and Level 2

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Normally you will not have to change the default value of this command.

This command applies only for the designated router or a specified interface. Only designated routers send CSNP packets in order to maintain database synchronization. The CSNP interval can be configured independently for Level 1 and Level 2.

The **isis csnp-interval** command on point-to-point subinterfaces should be used only in combination with the IS-IS mesh-group feature.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example configures Ethernet interface 2/5 for sending CSNPs every 30 seconds:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis csnp-interval 30 level-1
switch(config-if)#
```

Related Commands

show isis interface	Displays IS-IS information.

Send document comments to nexus7k-docfeedback@cisco.com

isis hello padding

To reenable Intermediate System-to-Intermediate System (IS-IS) hello padding at the interface level, enter the **isis hello padding** command. To disable IS-IS hello padding, use the **no** form of this command.

isis hello padding

no isis hello padding

Syntax Description

This command has no arguments or keywords.

Command Default

IS-IS hello padding is enabled.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding in order to avoid wasting network bandwidth in case the MTU of both interfaces is the same or, in case of translational bridging. While hello padding is disabled, Cisco routers still send the first five IS-IS hellos padded to the full MTU size, in order to maintain the benefits of discovering MTU mismatches.

To selectively disable hello padding for a specific interface, enter the **no isis hello padding** command in interface configuration mode. To disable hello padding for all interfaces on a router for the IS-IS routing process, enter the **no hello padding** command in router configuration mode.

This command requires the Enterprise Services license.

Examples

To turn off hello padding at the interface level for the Ethernet interface 0/0, enter the **no isis hello padding** command in interface configuration mode:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 0/0
switch(config-if)# no isis hello padding
switch(config-if)#
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
hello padding	Reenables IS-IS hello padding at the router level.

Send document comments to nexus7k-docfeedback@cisco.com

isis hello-interval

To specify the length of time between hello packets that the Cisco NX-OS software sends, use the **isis hello-interval** command. To restore the default value, use the **no** form of this command.

```
isis hello-interval seconds {level-1 | level-2}

no isis hello-interval {level-1 | level-2}
```

Syntax Description

<i>seconds</i>	Length of time between hello packets, in seconds. By default, a value three times the hello interval <i>seconds</i> is advertised as the hold time in the hello packets sent. (Change the multiplier of 3 by specifying the isis hello-multiplier command.) With smaller hello intervals, topological changes are detected faster, but there is more routing traffic. Range: 0 to 65535. Default: 10.
 Note On designated intermediate system (DIS) interfaces, only one third of the configured value is used. The full value of the configured hello intervals is used only by non-DIS interfaces.	
level-1	Configures the hello interval for Level 1 independently. Use this on X.25, Switched Multimegabit Data Service (SMDS), and Frame Relay multiaccess networks.
level-2	Configures the hello interval for Level 2 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.

Command Default

- The default settings are as follows:
- 10 seconds
 - Level 1 and Level 2

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The hello interval multiplied by the hello multiplier equals the hold time.

The hello interval can be configured independently for Level 1 and Level 2. The **level-1** and **level-2** keywords are used on LAN interfaces.

Send document comments to nexus7k-docfeedback@cisco.com

A faster hello interval gives faster convergence, but increases bandwidth and CPU usage. It might also add to instability in the network. A slower hello interval saves bandwidth and CPU usage. Especially when used in combination with a higher hello multiplier, configuration of the slower hello interval may increase overall network stability. When the hello interval is configured on DIS interfaces, only one third of the interval value is used. Therefore, the hold time (hello interval multiplied by the hello multiplier) for DIS interfaces will also be one third the hold time for non-DIS interfaces.

It makes more sense to tune the hello interval and hello multiplier on point-to-point interfaces than on LAN interfaces.

This command requires the Enterprise Services license.

Examples

The following example configures the Ethernet interface 2/3 to advertise hello packets every 5 seconds. The router is configured to act as a station router. This configuration will cause more traffic than the traffic generated by configuring a longer interval, but topological changes will be detected earlier.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/3
switch(config-if)# isis hello-interval 5 level-1
switch(config-if)#
```

Related Commands

Command	Description
isis hello-multiplier	Specifies the number of IS-IS hello packets that a neighbor must miss before the router should declare the adjacency as down.

Send document comments to nexus7k-docfeedback@cisco.com

isis hello-multiplier

To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the **isis hello-multiplier** command. To restore the default value, use the **no** form of this command.

isis hello-multiplier *multiplier* {**level-1** | **level-2**}

no isis hello-multiplier {**level-1** | **level-2**}

Syntax Description

<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.
level-1	Configures the hello multiplier independently for Level 1 adjacencies.
level-2	Configures the hello multiplier independently for Level 2 adjacencies.

Command Default

The default settings are as follows:

- *multiplier*: 3
- Level 1 and Level 2

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The “holding time” carried in an IS-IS hello packet determines how long a neighbor waits for another hello packet before declaring the neighbor to be down. This time determines how quickly a failed link or neighbor is detected so that routes can be recalculated. The advertised hold time in IS-IS hello packets will be set to the hello multiplier times the hello interval. Neighbors will declare an adjacency to this router down after not having received any IS-IS hello packets during the advertised hold time. The hold time (and thus the hello multiplier and the hello interval) can be set on a per-interface basis, and can be different between different routers in one area.

Using a smaller hello multiplier will give fast convergence, but can result in more routing instability. Increment the hello multiplier to a larger value to help network stability when needed. Never configure a hello multiplier lower than the default value of 3.

Use the **isis hello-multiplier** command in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval (**isis hello-interval** command) correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

Send document comments to nexus7k-docfeedback@cisco.com

On point-to-point links, there is only one hello for both Level 1 and Level 2, so different hello multipliers should be configured only for multiaccess networks such as Ethernet and FDDI. Separate Level 1 and Level 2 hello packets are also sent over nonbroadcast multiaccess (NBMA) networks in multipoint mode, such as X.25, Frame Relay, and ATM. However, we recommend that you run IS-IS over point-to-point subinterfaces over WAN NBMA media.

This command requires the Enterprise Services license.

Examples

In the following example, the network administrator wants to increase network stability by making sure an adjacency will go down only when many (ten) hello packets are missed. The total time to detect link failure is 60 seconds. This configuration will ensure that the network remains stable, even when the link is fully congested.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/3
switch(config-if)# ip router isis
switch(config-if)# isis hello-interval 6 level-1
switch(config-if)# isis hello-multiplier 10 level-1
```

Related Commands

Command	Description
isis hello-interval	Specifies the length of time between hello packets that the Cisco NX-OS software sends.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

isis lsp-interval

To configure the time delay between successive Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) transmissions, use the **isis lsp-interval** command. To restore the default value, use the **no** form of this command.

isis lsp-interval *milliseconds*

no isis lsp-interval

Syntax Description

<i>milliseconds</i>	Time delay between successive LSPs (in milliseconds). Range: 10 to 65535.

Command Default

The default time delay is 33 milliseconds.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

In topologies with a large number of IS-IS neighbors and interfaces, a router may have difficulty with the CPU load imposed by LSP transmission and reception. This command allows the LSP transmission rate (and the reception rate of other systems) to be reduced.

This command requires the Enterprise Services license.

Examples

The following example causes the system to send LSPs every 100 milliseconds (10 packets per second) on Ethernet interface 0/0:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 0/0
switch(config-if)# isis lsp-interval 100
```

Related Commands

Command	Description
isis retransmit-interval	Configures the time between retransmission of each LSP (IS-IS link-state PDU) over point-to-point links.

Send document comments to nexus7k-docfeedback@cisco.com

isis mesh-group

To optimize link-state packet (LSP) flooding in nonbroadcast multiaccess (NBMA) networks with highly meshed, point-to-point topologies, use the **isis mesh-group** command. To remove a subinterface from a mesh group, use the **no** form of this command.

isis mesh-group {*number* | **blocked**}

no isis mesh-group {*number* | **blocked**}

Syntax Description	<i>number</i>	Number identifying the mesh group of which this interface is a member. Range: 1 to 4294967295.
	blocked	Specifies that no LSP flooding take place on this subinterface.

Command Default The interface performs normal flooding.

Command Modes Interface configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines The LSPs that are first received on subinterfaces that are not part of a mesh group are flooded to all other subinterfaces in the usual way.

The LSPs that are first received on subinterfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group. If you enter the **blocked** keyword on a subinterface, then a newly received LSP is not flooded out over that interface.

To minimize the possibility of incomplete flooding, you should allow unrestricted flooding over at least a minimal set of links in the mesh. Selecting the smallest set of logical links that covers all physical paths results in very low flooding, but less robustness. Ideally, you should select only enough links to ensure that LSP flooding is not detrimental to scaling performance, but enough links to ensure that under most failure scenarios no router will be logically disconnected from the rest of the network. In other words, blocking flooding on all links permits the best scaling performance, but there is no flooding. Permitting flooding on all links results in very poor scaling performance.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

In the following example six interfaces are configured in three mesh groups. LSPs received are handled as follows:

- LSPs received first through Ethernet 1/0.1 are flooded to all interfaces except Ethernet 1/0.2 (which is part of the same mesh group) and Ethernet 1/2.1, which is blocked.
- LSPs received first through Ethernet 1/1.2 are flooded to all interfaces except Ethernet 1/1.1 (which is part of the same mesh group) and Ethernet 1/2.1, which is blocked.
- LSPs received first through Ethernet 1/2.1 are not ignored, but flooded as usual to all interfaces. LSPs received first through Ethernet 1/2.2 are flooded to all interfaces, except Ethernet 1/2.1, which is blocked.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/0.1
switch(config-if)# isis mesh-group 10
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/0.2
switch(config-if)# isis mesh-group 10
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/1.1
switch(config-if)# isis mesh-group 11
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/1.2
switch(config-if)# isis mesh-group 11
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/2.1
switch(config-if)# isis mesh-group blocked
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/2.2
switch(config-if)# isis mesh-group 12
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

Send document comments to nexus7k-docfeedback@cisco.com

isis metric

To configure the value of an Intermediate System-to-Intermediate System (IS-IS) metric, use the **isis metric** command. To restore the default metric value, use the **no** form of this command.

isis metric *metric-value* {**level-1** | **level-2**}

no isis metric *metric-value* {**level-1** | **level-2**}

Syntax Description		
	<i>metric-value</i>	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. Range: 1 to 16777215. Default: 10.
	maximum	Excludes a link or adjacency from the shortest path first (SPF) calculation.
	level-1	Specifies that this metric should be used only in the SPF calculation for Level 1 (intraarea) routing. If you do not specify an optional keyword, the metric is enabled on routing Level 1 and Level 2.
	level-2	Specifies that this metric should be used only in the SPF calculation for Level 2 (interarea) routing. If you do not specify a level, the metric is enabled on routing Level 1 and Level 2.

Command Default The default metric value is set to 10.

Command Modes Interface configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

Specifying the **level-1** or **level-2** keyword resets the metric only for Level 1 or Level 2 routing, respectively.

We recommend that you configure metrics on all interfaces. If you do not configure metrics on all interfaces, the IS-IS metrics are similar to hop-count metrics.

We recommend that you use the **metric-style wide** command to configure IS-IS to use the new-style type, length, value (TLV) because TLVs that are used to advertise IPv4 information in link-state packets (LSPs) are defined to use only expanded metrics. The Cisco NX-OS software provides support of a 24-bit metric field, the 24-bit metric field is called the *wide metric*. Using the new metric style, link metrics now have a maximum value of 16777215 with a total path metric of 4261412864.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example configures Ethernet interface 3/2 for a link-state metric cost of 15 for Level 1:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
switch(config-if)# isis metric 15 level-1
```

Related Commands

Command	Description
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style TLVs.

Send document comments to nexus7k-docfeedback@cisco.com

isis passive

To suppress adjacency forming on the interface, but still advertise the prefix associated with the interface, use the **isis passive** command. To disable suppression, use the **no** form of this command.

isis passive {**level-1** | **level-1-2** | **level-2-only**}

no isis passive {**level-1** | **level-1-2** | **level-2-only**}

Syntax Description	level-1	Suppresses Level 1 PDU only.
	level-1-2	Suppresses Level 1 and Level 2 PDU.
	level-2-only	Suppresses Level 2 PDU only.

Defaults

The default settings are as follows:

- This command is disabled by default.
- If enabled, the default is **level-1-2**.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is not necessary on a loopback interface. Use the **ip router isis** command in interface configuration mode on a loopback interface to associate that interface with the IS-IS instance.

This command requires the Enterprise Services license.

Examples

The following example suppresses adjacency for Ethernet interface 3/2 at Level 1:

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
switch(config-if)# isis passive level-1
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

isis priority

To configure the priority of designated routers, use the **isis priority** command in interface configuration mode. To reset the default priority, use the **no** form of this command.

isis priority *number-value* [**level-1** | **level-2**]

no isis priority [**level-1** | **level-2**]

Syntax Description

<i>number-value</i>	Sets the priority of a router and is a number from 0 to 127. The default value is 64.
level-1	(Optional) Sets the priority for Level 1 independently.
level-2	(Optional) Sets the priority for Level 2 independently.

Defaults

Priority of 64
Level 1 and Level 2

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Priorities can be configured for Level 1 and Level 2 independently. Specifying the **level-1** or **level-2** keyword resets priority only for Level 1 or Level 2 routing, respectively.

The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.

In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.

This command requires the Enterprise Services license.

Examples

The following example shows Level 1 routing given priority by setting the priority level to 80. This router is now more likely to become the DIS.

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
```

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config-if)# isis priority 80 level-1
```

 isis priority

Send document comments to nexus7k-docfeedback@cisco.com



L Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter L.

load-balancing

To specify the load-balancing method used by the active virtual gateway (AVG) of the Gateway Load Balancing Protocol (GLBP), use the **load-balancing** command. To disable load balancing, use the **no** form of this command.

load-balancing [**host-dependent** | **round-robin** | **weighted**]

no load-balancing

Syntax Description	host-dependent	(Optional) Specifies a load-balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged.
	round-robin	(Optional) Specifies a load-balancing method where each virtual forwarder is included in Address Resolution Protocol (ARP) replies for the virtual IP address. This method is the default.
	weighted	(Optional) Specifies a load-balancing method that is dependent on the weighting value advertised by the gateway.

Defaults	The round-robin method is the default.

Command Modes	GLBP configuration

Supported User Roles	Network Administrator VDC Administrator

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the host-dependent method of GLBP load balancing when you need each host to always use the same router. Use the weighted method of GLBP load balancing when you need unequal load balancing because gateways in the GLBP group have different forwarding capacities.

This command does not require a license.

Examples

The following example show how to configure the host-dependent load-balancing method for the AVG of the GLBP group 10:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# load-balancing host-dependent
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
show glbp	Displays GLBP information.
weighting	Configures the weighting value and thresholds for the weighted load-balancing method.
weighting track	Configures object tracking for the weighted load-balancing method.

Send document comments to nexus7k-docfeedback@cisco.com

local-as

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

local-as *as-number*

Syntax Description	<i>as-number</i> (Optional) The 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>.

Defaults	None

Command Modes	Router VRF mode

Supported User Roles	network-admin vdc-admin

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	This example shows how to configure the local AS number for BGP: <pre>switch# config t switch(config)# router bgp 65536.33 switch(config-router)# vrf red switch(config-router-vrf)# local-as 65536.33</pre>

Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show bgp</td><td>Displays information about BGP.</td></tr></table>	Command	Description	show bgp	Displays information about BGP.
Command	Description				
show bgp	Displays information about BGP.				

Send document comments to nexus7k-docfeedback@cisco.com

log-adjacency-changes (EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) adjacency state, use the **log-adjacency-changes** command. To disable the logging of changes in 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.

Defaults

Adjacency changes are not logged.

Command Modes

Address-family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to enable logging of adjacency state changes for EIGRP 1:

```
switch(config)# router eigrp 1
switch(config-router)# address-family ipv6
switch(config-router-af)# log-adjacency-changes
```

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.

Send document comments to nexus7k-docfeedback@cisco.com

log-adjacency-changes (IS-IS)

To enable the router to send a syslog message when an Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) neighbor goes up or down, use the **log-adjacency-changes** configuration mode command. To disable this function, 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	This command is enabled by default.

Command Modes	Router configuration VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	The log-adjacency-changes command is on by default but only up/down (full/down) events are reported.

Examples	The following example configures the router to send a syslog message when an IS-IS neighbor state changes:

```
switch(config)# router isis  
switch(config-router)# log-adjacency-changes
```

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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	Provides all (DOWN, INIT, 2WAY, EXSTART, EXCHANGE, LOADING, FULL) adjacency state changes.
Defaults	The router sends a system message when the state of an OSPF neighbor changes.	
Command Modes	Router configuration Router VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following example shows how to configure the router to send a system message when an OSPF neighbor state changes: <pre>switch(config)# router ospf 209 switch(config-router)# log-adjacency-changes detail</pre>	

Send document comments to nexus7k-docfeedback@cisco.com

log-adjacency-changes (OSPFv3)

To configure the router to send a system message when the state of an Open Shortest Path First version 3 (OSPFv3) 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	Provides all (DOWN, INIT, 2WAY, EXSTART, EXCHANGE, LOADING, FULL) adjacency state changes.

Defaults	The router sends a system message when the state of an OSPFv3 neighbor changes.

Command Modes	Router configuration Router VRF configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the log-adjacency-changes command to display high-level changes to the state of the OSPFv3 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 Enterprise Services license.

Examples	This example shows how to configure the router to send a system message when an OSPFv3 neighbor state changes: switch(config)# router ospfv3 209 switch(config-router)# log-adjacency-changes detail

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

Syntax Description	<i>seconds</i>	(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 Router configuration Router VRF configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(3)	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 Enterprise Services license.

Examples	The following 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
```

Related Commands	Command	Description
	log-adjacency-changes	Enables logging of EIGRP adjacency state changes.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults	Some eBGP peers shut down for severe memory alerts.

Command Modes	Neighbor configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following 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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

lsp-gen-interval

To customize the IS-IS throttling of the LSP generation, use the **lsp-gen-interval** configuration mode command. To restore default values, use the **no** form of this command.

lsp-gen-interval {**level-1** | **level-2**} *lsp-max-wait* [*lsp-initial-wait* *lsp-second-wait*]

no lsp-gen-interval

Syntax Description

level-1	Applies intervals to level-1 areas only.
level-2	Applies intervals to level-2 areas only.
<i>lsp-max-wait</i>	Maximum interval (in seconds) between two consecutive occurrences of an LSP being generated. Range: 500 to 65535. Default: 5.
<i>lsp-initial-wait</i>	(Optional) Initial LSP generation delay (in milliseconds). Range: 50 to 65535. Default: 50.
<i>lsp-second-wait</i>	Hold time between the first and second LSP generation (in milliseconds). Range: 50 to 65535. Default: 50.

Command Default

The defaults are as follows:

- *lsp-max-wait*: 500
- *lsp-initial-wait*: 50
- *lsp-second-wait*: 50

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When you change the default values of this command, use the following guidelines:

- The *lsp-initial-wait* argument indicates the initial wait time (in milliseconds) before generating the first LSP.
- The *lsp-second-wait* argument indicates the amount of time to wait (in milliseconds) between the first and second LSP generation.

Send document comments to nexus7k-docfeedback@cisco.com

- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the **lsp-max-wait** interval specified, so this value causes the throttling or slowing down of the LSP generation after the initial and second intervals. Once this interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for 2 times the **lsp-max-wait** interval, fast behavior is restored (the initial wait time).

The **lsp-mtu** command sets the delay (in milliseconds) between successive LSPs being transmitted (including LSPs generated by another system and forwarded by the local system).

You can enter these commands in combination to control the rate of LSP packets being generated, transmitted, and retransmitted.

Examples

The following example configures the interval for LSP generation:

```
switch(config)# router isis  
switch(config-router)# lsp-gen-interval 2 50 100
```

Related Commands

Command	Description
exit	Exits the current configuration mode.
feature isis	Enables IS-IS on the router.
no	Negates a command or sets its defaults.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

lsp-mtu

To set the maximum size of a link-state packet (LSP) generated by Cisco NX-OS software, use the **lsp-mtu** configuration mode command. To restore the default Maximum Transmission Unit (MTU) size, use the **no** form of this command.

lsp-mtu *bytes*

no lsp-mtu

Syntax Description

bytes Maximum LSP size in bytes. Range: 128 to 4352. Default: 1492.

Command Default

The default MTU size is 1492 bytes.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can increase the LSP MTU if there is a very large amount of information generated by a single router, because each device is limited to approximately 250 LSPs. In practice, this should never be necessary.

The LSP MTU must never be larger than the smallest MTU of any link in the area. This is because LSPs are flooded throughout the area.

The **lsp-mtu** command limits the size of LSPs generated by this router only.

Examples

The following example sets the maximum LSP size to 1500 bytes:

```
switch(config)# router isis
switch(config-router)# lsp-mtu 1500
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com



M Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter M.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

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

Defaults

None

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

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 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. .

This command does not require a license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

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, or enables policy routing.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

match as-path

To match a BGP autonomous system path access list, use the **match as-path** command in route-map configuration mode. 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

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

Defaults

No path lists are defined.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

This command does not require a license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

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, and performs policy routing on packets.
	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.
	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, or enables policy routing.
	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 vrf	Sets the VRF for next-hop resolution.
	set weight	Specifies the BGP weight for the routing table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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.

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

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

Syntax Description

<i>name</i>	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 (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some 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.

This command does not require a license.

Examples

The following example shows how to match two BGP communities:

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


Send document comments to nexus7k-docfeedback@cisco.com

The following example shows that the routes matching community list 1 will have the weight set to 200. Any route that has the standard community 109 only will have 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
```

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

```
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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

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

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

Syntax Description

<i>name</i>	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 (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(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 will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some 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.

This command does not require a license.

Examples

The following example shows how to match two BGP extended community lists:

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

Send document comments to nexus7k-docfeedback@cisco.com

The following example shows that the routes that match the extended community list bgpLocal will 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
```

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

Syntax Description

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

Defaults

None

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **match interface** command to provide a list of interfaces to match a route against. Route next-hop addresses that are reached by one of these 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 relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

This command does not require a license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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, or to perform policy routing on packets, use the **match ip address** command in route-map configuration mode. To remove the **match ip address** entry, use the **no** form of this command.

```
match ip address { access-list-name [access-list-name...] | prefix-list prefix-list-name
[prefix-list-name...] }
```

```
no match ip address { access-list-name [access-list-name...] | prefix-list prefix-list-name
[prefix-list-name...] }
```

Syntax Description

<i>access-list-name...</i>	Name of a standard or expanded access 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.
prefix-list <i>prefix-list-name...</i>	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.

Defaults

No access list names or prefix lists are specified.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The *access-list-name* argument is supported in route-maps for PBR only.

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

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 or to subject packets to policy routing. Both purposes are described in this section.

Send document comments to nexus7k-docfeedback@cisco.com

Redistribution

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 sections that contain specific **match** clauses. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Policy Routing

Another purpose of route maps is to enable policy routing. The **match ip address** command allows you to policy route packets based on criteria that can be matched with an expanded access list; for example, a protocol, protocol service, and source or destination IP address. To define the conditions for policy routing packets, use the **ip policy route-map** interface configuration command, in addition to the **route-map** global configuration command, and the **match** and **set** route-map configuration commands. 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 policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets based on their source, for example, using an access list.

This command does not require a license.

Examples

In the following example, routes that have addresses specified by access list test will be matched:

```
switch(config)# feature pbr
switch(config)# interface ethernet 2/10
switch(config-if)# ip policy route-map chicago
switch(config-if)# exit
switch(config)# route-map chicago
switch(config-route-map)# match ip address test
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
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, or enables policy routing.
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 ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

match ip multicast

To configure the IPv4 multicast features for the route-map matching, use the **match ip multicast** route-map configuration 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** | **bidir**}]}

no match ip multicast

Syntax Description

group <i>address/length</i>	Specifies the group address and the length of the network mask in bits, in this format: <i>A.B.C.D/length</i> . 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 <i>address/length</i>	Specifies the source address and the length of the network mask in bits, in this format: <i>A.B.C.D/length</i> . 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 <i>address/length</i>	Specifies the IPv4 rendezvous prefix (RP) and the length of the IPv4 prefix mask in bits, in this format: <i>A.B.C.D/length</i> . 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	Specifies the any-source multicast (ASM) rendezvous point type.
bidir	Specifies the bidirectional (bidir) multicast rendezvous point type.

Command Default

None

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Added source keyword.

Usage Guidelines

To specify the multicast attributes to match, use 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:

Send document comments to nexus7k-docfeedback@cisco.com

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

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

You can configure both group and rp options.

This command does not require a license.

Examples

This examples 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 examples shows how to specify both the group IPv4 prefix and the rendezvous point 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
ip policy route-map	Identifies a route map to use for policy routing on an interface.
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 length	Bases policy routing on the Level 3 length of a packet.
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, or enables policy routing.
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 ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set level	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 in route-map configuration mode. 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

<i>prefix-list-name</i>	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 (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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.

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 relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Send document comments to nexus7k-docfeedback@cisco.com

This command does not require a license.

Examples

The following example distributes routes that have a next hop router address passed by prefix list test will be distributed:

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

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, and performs policy routing on packets.
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, or enables policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 in route-map configuration mode. 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

<i>prefix-list-name</i>	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.

Defaults

No filtering on route source.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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.

Send document comments to nexus7k-docfeedback@cisco.com

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be 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.

This command does not require a license.

Examples

The following example distributes 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, and performs policy routing on packets.
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, or enables policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

match ipv6 address

To distribute any routes that have a destination IPv6 network number address that is permitted by a standard access list, an expanded access list, or a prefix list, or to perform policy routing on packets, use the **match ipv6 address** command in route-map configuration mode. To remove the **match** statement from the route map, use the **no** form of this command.

match ipv6 address {**prefix-list** *prefix-list-name* [*prefix-list-name...*] | *access-list-name*

no match ipv6 address {**prefix-list** *prefix-list-name* [*prefix-list-name...*] | *access-list-name*}

Syntax Description

<i>access-list-name...</i>	Name of a standard or expanded access list. It can be any alphanumeric string up to 63 characters. You can only use access lists for policy-based routing.
prefix-list <i>prefix-list-name...</i>	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. You can configure up to 32 prefix lists.

Defaults

No access list names or prefix lists are specified.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The *access-list-name* argument is supported in route-maps for PBR only.

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 or to subject packets to policy routing. Both purposes are described in this section.

Send document comments to nexus7k-docfeedback@cisco.com

Redistribution

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 sections that contain specific **match** clauses. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

This command does not require a license.

Examples

In the following example, routes that have addresses specified by access list name red will be matched:

```
switch(config)# feature pbr
switch(config)# route-map blue
switch(config-route-map)# match ipv6 address red
```

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 length	Bases policy routing on the Level 3 length of a packet.
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, or enables policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

match ipv6 multicast

To configure the IPv6 multicast features for the route-map matching, use the **match ipv6 multicast** route-map configuration command. To remove the match, use the **no** form of this command.

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

Syntax Description	
group <i>address/length</i>	Specifies the group address and the length of the network mask in bits, in this format: <i>A:B::C:D/length</i> . The network number can be any valid IPv6 address or prefix. The range for <i>length</i> is 0 to 0x7FFFFFFF. You can specify the group , source , and rp options.
source <i>address/length</i>	Specifies the source address and the length of the network mask in bits, in this format: <i>A:B::C:D/length</i> . The network number can be any valid IPv6 address or prefix. The range for <i>length</i> is 0 to 0x7FFFFFFF. You can specify the group , source , and rp options.
rp <i>address/length</i>	Specifies the IPv6 rendezvous prefix (RP) and the length of the IPv6 prefix mask in bits, in this format: <i>A:B::C:D/length</i> . The network number can be any valid IPv6 address or prefix. The bit mask can be a number from 0 to 32. You can specify the group , source , and rp options.
rp-type	(Optional) Specifies the multicast rendezvous point type.
asm	Specifies the any-source multicast (ASM) rendezvous point type.
bidir	Specifies the bidirectional (bidir) multicast rendezvous point type.

Command Default	None

Command Modes	Route-map configuration (config-route-map)

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added the source keyword.

Usage Guidelines	To specify the multicast attributes to match, use the match ipv6 multicast route-map configuration command. You must enter the feature pbr global configuration mode command to enable PBR before entering the route-map command.

Send document comments to nexus7k-docfeedback@cisco.com

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 ipv6 multicast** command.

You can specify the **group**, **source**, and **rp** options.

This command does not require a license.

Examples

This examples shows how to specify the group IPv6 prefix and the length of the IPv6 prefix for the neighbors to match:

```
switch(config)# route-map blueberry
switch(config-route-map)# match ipv6 multicast group 30:0::0:0/12
switch(config-route-map)#
```

This examples shows how to specify both the group IPv6 prefix and the rendezvous point IPv6 prefix for the neighbors to match:

```
switch(config)# route-map red
switch(config-route-map)# match ipv6 multicast group 30:0::0:0/12 rp 2001:0DB8::/48
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 ipv6 next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ipv6 route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
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, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set ipv6 default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.
set ipv6 next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

match ipv6 next-hop prefix-list

To redistribute any IPv6 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 in route-map configuration mode. To remove the next hop entry, use the **no** form of this command.

match ipv6 next-hop prefix-list *name* [...*name*]

no match ipv6 next-hop prefix-list *name* [...*name*]

Syntax Description

<i>name</i> ...	Prefix list name. 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 (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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



Note

A permit route map containing only **set** commands and no **match** commands permits all routes.

Send document comments to nexus7k-docfeedback@cisco.com

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 relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

This command does not require a license.

Examples

The following example distributes routes that have a next hop router address passed by prefix list 5 will be distributed:

```
switch(config)# route-map blue
switch(config-route-map)# match ipv6 next-hop prefix-list test
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 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 length	Bases policy routing on the Level 3 length of a packet.
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, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set ipv6 default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.
set ipv6 next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

match ipv6 route-source prefix-list

To redistribute IPv6 routes that have been advertised by routers and access servers at the address specified by the access lists, use the **match ipv6 route-source prefix-list** command in route-map configuration mode. To remove the route-source entry, use the **no** form of this command.

match ipv6 route-source prefix-list *name* [...*name*]

no match ipv6 route-source prefix-list *name* [...*name*]

Syntax Description

<i>name</i> ...	Prefix list name. It can be any alphanumeric string up to 63 characters. The ellipsis indicates that multiple values can be entered, up to 32 prefix lists.

Defaults

No filtering on route source.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Send document comments to nexus7k-docfeedback@cisco.com

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be 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.

This command does not require a license.

Examples

The following example distributes routes that have been advertised by routers and access servers at the addresses specified by prefix list test:

```
switch(config)# route-map blue
switch(config-route-map)# match ipv6 route-source prefix-list test
```

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, and performs policy routing on packets.
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, or enables policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

match length

To base policy routing on the Level 3 length of a packet, use the **match length** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match length *minimum-length maximum-length*

no match length *minimum-length maximum-length*

Syntax Description

<i>minimum-length</i>	Minimum Level 3 length of the packet, inclusive, allowed for a match. Range: 0 to 2147483647.
<i>maximum-length</i>	Maximum Level 3 length of the packet, inclusive, allowed for a match. Range: 0 to 2147483647.

Command Default

No policy routing occurs on the length of a packet.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

In IPv4, use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In IPv4, 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 packet to be routed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

In IPv4, you might want to base your policy routing on the length of packets so that your interactive traffic and bulk traffic are directed to different routers.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to set the packets 3 to 200 bytes long:

```
switch(config)# route-map blue
switch(config-route-map)# match length 3 200
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

match route-type

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

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

no match route-type { **external** | **internal** | **level-1** | **level-2** | **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.
level-1	Specifies the Intermediate System-to-Intermediate System (IS-IS) level-1 route. You can specify more than one keyword.
level-2	Specifies the IS-IS level-2 route. 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.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

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 relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be 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.

You can specify more than one keyword.

This command does not require a license.

Examples

The following example redistributes internal routes:

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

The following example redistributes 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 address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
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, or enables policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
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.

Send document comments to nexus7k-docfeedback@cisco.com

match tag

To redistribute routes in the routing table that match the specified tags, use the **match tag** command in route-map configuration mode. 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	<i>tag-value</i> List of one or more route tag values. Each can be an integer from 0 to 4294967295. You can configure up to 32 tags.					
Defaults	No match tag values are defined.					
Command Modes	Route-map configuration (config-route-map)					
Supported User Roles	network-admin vdc-admin					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(1)	This command was introduced.
Release	Modification					
4.0(1)	This command was introduced.					
Usage Guidelines	An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the <i>tag-value</i> 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 <i>match criteria</i>—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the <i>set actions</i>—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 <i>set actions</i> 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 relating to a route-map command will be ignored; that is, the route will not be advertised for outbound route maps and will not be 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. This command does not require a license.					

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example redistributes routes stored in the routing table with tag 5:

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

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, and performs policy routing on packets.
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, or enables policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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.
	<i>seconds</i>	(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.

Defaults	Originates router link-state advertisements (LSAs) with normal link metrics.

Command Modes	Router configuration Router VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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, which allows 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:

Send document comments to nexus7k-docfeedback@cisco.com

- 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.
- Introducing a router into a network without routing traffic through it. You may 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.
- Gracefully removing a router from a network. This feature allows you to gracefully remove a router from the network by advertising a maximum metric through all links, which allows other routers to select alternate paths for transit traffic to follow before the router is shut down.


Note

You should not save the running configuration of a router that is configured for a graceful shutdown because the router will continue to advertise a maximum metric after it is reloaded.

This command requires the Enterprise Services license.

Examples

The following 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
```

The following 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
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.

Send document comments to nexus7k-docfeedback@cisco.com

max-lsp-lifetime

To set the maximum time for which link-state packets (LSPs) persist without being refreshed, use the **max-lsp-lifetime** configuration mode command. To restore the default time, use the **no** form of this command.

max-lsp-lifetime *value*

no max-lsp-lifetime

Syntax Description	<i>value</i> (Optional) Maximum LSP lifetime in seconds. Range: 1 to 65535. Default: 1200.

Command Default	The default is 1200 seconds.

Command Modes	Router configuration VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	The maximum LSP lifetime must be greater than the LSP refresh interval. This command requires the Enterprise Services license.

Command Default	The following example sets the maximum time that the LSP persists to 11,000 seconds (more than 3 hours): switch(config)# router isis switch(config-router)# max-lsp-lifetime 11000

Related Commands	Command	Description
	exit	Exits the current configuration mode.
	feature isis	Enables IS-IS on the router.
	no	Negates a command or sets its defaults.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>number</i> (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 VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.1(2)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Command Default	The following example shows how to set the maximum number of AS numbers to 50: <pre>switch(config)# router bgp 64496 switch(config-router)# maxas-limit 50</pre>	
Related Commands	Command	Description
	feature bgp	Enables the BGP feature.
	router bgp	Creates a BGP instance.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

maximum-paths (BGP)

To control the maximum number of parallel routes that the Border Gateway Protocol (BGP) can support, use the **maximum-paths** configuration mode 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	Configures the maximum interior BGP (iBGP) paths.
	<i>number-paths</i>	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	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	There are no usage guidelines for this command.	
Examples	The following example shows how to allow a maximum of 16 paths to a destination for a BGP routing process:	
	<pre>switch(config)# router bgp 64496 switch(config-router)# maximum-paths 16</pre>	
Related Commands	Command	Description
	feature bgp	Enables the BGP feature on the router.
	router bgp	Enables BGP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>maximum</i>	Maximum number of parallel routes that EIGRP can install in a routing table. The range is from 1 to 16 routes.

Defaults

8 paths

Command Modes

Address-family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(2)	The default maximum paths was changed to 8 from 16.

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 are equal cost (according to the EIGRP best path algorithm).

This command requires the Enterprise Services license.

Examples

The following example shows how to allow a maximum of 10 paths to a destination:

```
switch(config)# router eigrp 1
switch(config-router)# maximum-paths 10
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

maximum-paths (IS-IS)

To control the maximum number of parallel routes that an IP routing protocol can support, use the **maximum-paths** configuration mode command. To restore the default number of parallel routes, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description	<i>number-paths</i> 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 configuration VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	There are no usage guidelines for this command.	
Examples	The following example shows how to allow a maximum of 16 paths to a destination for an IS-IS routing process: <pre>switch(config)# router isis 3 switch(config-router)# maximum-paths 16</pre>	
Related Commands	Command	Description
	exit	Exits the current configuration mode.
	feature isis	Enables IS-IS on the router.
	no	Negates a command or sets its defaults.
	router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

maximum-paths (RIP)

To configure the maximum number of equal cost parallel routes that the the Routing Information Protocol (RIP) will install into the routing table, use the **maximum-paths** command in the router address-family configuration mode. To remove the **maximum-paths** command and restore the system to its default condition with respect to RIP, use the **no** form of this command.

maximum-paths *maximum*

no maximum-paths

Syntax Description	<i>maximum</i> Maximum number of parallel routes that RIP can install in a routing table. The range is from 1 to 16.	
Defaults	8 paths	
Command Modes	Router address-family configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	The following example shows how to allow a maximum of 16 equal cost paths to a destination: <pre>switch(config)# router rip Enterprise switch(config-router)# address-family ipv4 unicast switch(config-router-af)# maximum-paths 16</pre>	
Related Commands	Command	Description
	address-family	Enters address-family configuration mode.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>maximum</i>	Maximum number of parallel routes that OSPF can install in a routing table. The range is from 1 to 16 routes.
Defaults	8 paths	
Command Modes	Router configuration Router VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following example shows how to allow a maximum of 10 paths to a destination: switch(config)# router ospf 1 switch(config-router)# maximum-paths 10	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

maximum-paths (OSPFv3)

To control the maximum number of parallel routes that Open Shortest Path First version 3 (OSPFv3) 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

<i>maximum</i>	Maximum number of parallel routes that OSPFv3 can install in a routing table. The range is from 1 to 16 routes.

Defaults

8 paths

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **maximum-paths** command to allow OSPFv3 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 OSPFv3 shortest path first algorithm).

This command requires the Enterprise Services license.

Examples

This example shows how to allow a maximum of 10 paths to a destination:

```
switch(config)# router ospfv3 1
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# maximum-paths 10
```

Send document comments to nexus7k-docfeedback@cisco.com

maximum-prefix

To control how many prefixes can be received from a neighbor, use the **maximum-prefix** command in peer template configuration mode. 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	<i>maximum</i>	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.
	<i>threshold</i>	(Optional) Integer specifying at what percentage of the maximum-prefix limit the router starts to generate a warning message. Range: 1 to 100. Default: 75.
	restart <i>interval</i>	(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 will stay down after the maximum-prefix limit is exceeded.

Command Modes	Peer template configuration Router bgp configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 will accept 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.

Send document comments to nexus7k-docfeedback@cisco.com

When the number of received prefixes exceeds the maximum number configured, BGP disables the peering session (by default). If the **restart** keyword is configured, BGP will automatically reestablish the peering session at the configured time interval. If the **restart** keyword is not configured and a peering session is terminated because the maximum prefix limit has been exceeded, the peering session will not be reestablished until the **clear ip bgp** command is entered. 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

In the following example, the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

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

In the following example, the maximum number of prefixes that will be 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(config)# router bgp 64496  
switch(config-router)# network 192.168.0.0  
switch(config-router)# maximum-prefix 5000 50
```

In the following example, the maximum number of prefixes that will be 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(config)# router bgp 64496  
switch(config-router)# network 192.168.0.0  
switch(config-router)# maximum-prefix 2000 restart 30
```

In the following example, warning messages will be 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
```

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>key-id</i>	Identifier in the range from 1 to 255.
	0	Specifies to use an unencrypted password to generate the md5 key.
	3	Specifies to use an encrypted 3DES password to generate the md5 key.
	<i>key</i>	Alphanumeric password of up to 16 bytes.
Defaults	Unencrypted	
Command Modes	Virtual link configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Use the message-digest-key command when you configure the MD5 digest authentication mode. Both interfaces on the virtual link must have the same <i>key</i> value. This command requires the Enterprise Services license.	
Examples	The following 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	
Related Commands	Command	Description
	authentication (virtual-link)	Configures the authentication mode on a virtual link.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>hops-number</i>	Maximum hop count. The range is from 1 to 255 hops.

Defaults

hops-number: 100

Command Modes

Address-family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **metric maximum-hops** command to provide a safety mechanism that causes EIGRP to advertise as unreachable routes with a hop count greater than the value assigned to the *hops-number* argument. This command requires the Enterprise Services license.

Examples

The following 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
```

Related Commands

Command	Description
metric weights	Tunes the EIGRP metric calculations.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>tos</i> <i>k1 k2 k3 k4 k5</i> Type of service (ToS) which must always be zero. 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.	
Defaults	<i>tos</i>: 0 <i>k1</i>: 1 <i>k2</i>: 0 <i>k3</i>: 1 <i>k4</i>: 0 <i>k5</i>: 0	
Command Modes	Address-family configuration Router configuration Router VRF configuration	
SupportedUserRoles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 ToS. If k5 equals 0, Cisco NX-OS computes the composite EIGRP metric according to the following formula:	

Send document comments to nexus7k-docfeedback@cisco.com

$$\text{metric} = [k1 \times \text{bandwidth} + (k2 \times \text{bandwidth}) / (256 - \text{load}) + k3 \times \text{delay}]$$

If k5 does not equal zero, Cisco NX-OS performs an additional calculation:

$$\text{metric} = \text{metric} \times [k5 / (\text{reliability} + k4)]$$

Use the **bandwidth** command in interface configuration mode to set the bandwidth metric.

Use the **delay** command in interface configuration mode to set the delay.

255 is a reliability of 100 percent or a perfectly stable link. A load of 255 indicates a completely saturated link.

This command requires the Enterprise Services license.

Examples

The following example shows how to set the metric weights to change the default values:

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# metric weights 0 2 0 2 0 0
```

Related Commands

Command	Description
bandwidth	Sets the EIGRP bandwidth metric in interface configuration mode.
delay	Sets the EIGRP delay metric in interface configuration mode.

Send document comments to nexus7k-docfeedback@cisco.com

metric-style transition

To configure the metric style that Intermediate-System-to-Intermediate System (IS-IS) uses in advertised link-state update messages (LSPs), use the **metric-style transition** command. To revert to the default setting, use the **no** form of this command.

metric-style transition

no metric-style transition

Syntax Description	This command has no keywords or arguments.

Command Default	Wide metric style

Command Modes	Router configuration VRF configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	Use the metric-style transition command to configure IS-IS to generate and accept both narrow metric style and wide metric style Type Length Value (TLV) objects. This command requires the Enterprise Services license.

Examples	The following example shows how to configure the metric style: <pre>switch(config-router)# metric-style transition switch(config-router)#</pre>

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Creates an IS-IS instance.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com



N Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter N.

Send document comments to nexus7k-docfeedback@cisco.com

neighbor

To configure a BGP neighbor (router, 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* | *ipv6-addr* | *ipv6-prefix/length*} [**remote-as** {*as-num* [*.as-num*] | **route-map** *name*}]

no neighbor {*ip-addr* | *ip-prefix/length* | *ipv6-addr* | *ipv6-prefix/length*} [**remote-as** {*as-num* [*.as-num*] | **route-map** *name*}]

Syntax Description

<i>ip-addr</i>	IP address of the neighbor in this format: A.B.C.D.
<i>ip-prefix/length</i>	IP prefix and the length of the IP prefix. The format is x.x.x.x/ <i>length</i> . The <i>length</i> range is from 1 to 32.
<i>ipv6-addr</i>	IPv6 address of the neighbor. The format is A:B::C:D.
<i>ipv6-prefix/length</i>	IPv6 prefix and the length of the IPv6 prefix for neighbors. The format is A:B::C:D/ <i>length</i> . The <i>length</i> range is from 1 to 128.
remote-as	(Optional) Specifies the autonomous system number of the neighbor.
<i>as-num</i>	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. The range is from 1 to 65535.
<i>.as-num</i>	(Optional) Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. The range is from 1 to 65535.
route-map <i>name</i>	(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

This command has no default settings.

Command Modes

Neighbor address-family configuration
Router bgp configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	Added support for the route-map keyword.
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Use the **neighbor** command to enter the BGP neighbor configuration mode. When you enter the **neighbor** command, the prompt changes to `switch(config-router-neighbor)#`.

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

- **address-family**—Configure 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 eBGP peer that is directly connected to the local router. BGP triggers a connection check automatically for all eBGP peers that are known to be 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 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.

You must use the **update-source** command to enable IPv6 link-local peering for internal or external BGP sessions.

Send document comments to nexus7k-docfeedback@cisco.com

This command requires the Enterprise Services license.

Examples

The following 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
```

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
```

The following 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
```

The following example shows how to source IPv6 BGP TCP connections for the specified neighbor in autonomous system 64496 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 64498 with the link-local IPv6 address of Ethernet interface 2/1:

```
switch(config)# router bgp 64497
switch(config-router)# neighbor 3ffe::3 remote-as 64496
switch(config-router-neighbor)# update-source Loopback0
switch(config-router-neighbor)# neighbor fe80::2 remote-as 64498
switch(config-router-neighbor)# update-source Ethernet 2/1
```

Related Commands

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

Send document comments to nexus7k-docfeedback@cisco.com

net

To configure an Intermediate System-to-Intermediate System (IS-IS) network entity (NET) for the routing process, use the **net** command in global configuration mode. To remove a NET, use the **no** form of this command.

net *net*

no net *net*

Syntax Description

<i>net</i>	NET network services access point (NSAP) name or address for the IS-IS routing process; see the “Usage Guidelines” section for additional information about valid values.

Command Default

The defaults are as follows:

- No NET is configured.
- The IS-IS process is disabled.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

An IS (intermediate system) is identified by an address known as a network access point (NASAP). The NSAP is divided up into three parts as specified by ISO/AI 10589:

- Area address—This field is of variable length, composed of high order octets, and it excludes the System ID and N-selector (NSEL) fields. This area address is associated with a single area within the routing domain.
- System ID—This field is 6 octets long and should be set to a unique value with level-1 and level 2. The system ID defines an end system (ES) or an IS in an area. You configure the area address and the system ID with the NET command. You can display the system ID with the `show isis topology` command.
- NSEL—This field is called the N-selector, also referred to as the NSAP, and it specifies the upper-layer protocol. The NSEL is the last byte of the NSAP and identifies a network service user. A network service user is a transport entity or the IS network entity itself. When the N-selector is set to zero, the entire NSAP is called a network entity title (NET).

Send document comments to nexus7k-docfeedback@cisco.com

A NET is an NSAP where the last byte is always the n-selector and is always zero. A NET can be from 8 to 20 bytes in length. The NET is formatted as follows: XX.AAAA.AAAA.AAAA[.AAAA].XX.

Under most circumstances, you should configure one NET only. It is possible to configure two or three NETs, but you should not configure more than one NET except for the following unusual circumstances:

- A network configuration has multiple areas that are merged.
- One area in the IS-IS process is being split into multiple areas.

Configuring multiple NETs in these two circumstances can be temporarily useful because multiple area addresses enable you to renumber an area individually as needed.

If you are using IS-IS to perform IP routing only (no connectionless network service routing is enabled), you must configure a NET to define the router ID and area ID.

Examples

The following example shows how to configure a router with a NET which consists of the system ID 0000.0c11.1110 and area address 47.0004.0(1)04d.0001:

```
switch(config)# router isis firstcompany
switch(config-router)# net 47.0004.0(1)04d.0001.00
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

network

To configure an IP prefix to advertise, use the **network** address family configuration mode 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	<i>ip-addr</i>	IP network address to advertise; use the following format: A.B.C.D.
	<i>ip-prefix/length</i>	IP prefix and the length of the IP prefix. The length of the IPv6 prefix is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. Use the following format: A.B.C.D/length.
	mask <i>mask-num</i>	Configures the mask of the IP prefix to advertise in dotted 4-octet format.
	route-map <i>name</i>	(Optional) Specifies the name of the route-map to modify attributes.

Command Default This command has no default settings.

Command Modes Neighbor address-family configuration
Router bgp configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines IP prefix to advertise is considered for bestpath and advertisement to peers only if a route of equal or more specificity is present in the routing table.

Examples The following 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) #
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

nexthop route-map

To specify that Border Gateway Protocol (BGP) routes are resolved using only next hops whose routes 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

<i>name</i>	Route map name . The name can be any alphanumeric string up to 63 characters.

Command Default

None

Command Modes

Address-family configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(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 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 Enterprise Services license.

Examples

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

```
switch# config t
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
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

nexthop trigger-delay

To specify that 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 <i>delay</i>	Specifies the critical next-hop trigger delay, in milliseconds. The range is from 0 to 4294967295. The default is 3000.
non-critical <i>delay</i>	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

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(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 at least equal or greater than 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 an Enterprise Services license.

Examples

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

```
switch# config t
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
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

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

Send document comments to nexus7k-docfeedback@cisco.com



0 Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter O.

object

o 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 t
```

Syntax Description	not	(Optional) Negates the state of an object.
	Note The not keyword cannot be used in a weight or percentage threshold list. It can only be used in a Boolean list.	
	weight weight-number	(Optional) Specifies a threshold weight for each object.

Defaults	None

Command Modes	tracking configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.2(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.

Send document comments to nexus7k-docfeedback@cisco.com

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%, two of the objects must be in the up state (66% 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.

This command does not require a license.

Examples

The following 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
switch(config-track)# object 30
```

Related Commands

Command	Description
track list	Configures a track list for object tracking.

Send document comments to nexus7k-docfeedback@cisco.com

ospfv3 cost

To specify the cost of sending a packet on an interface, use the **ospfv3 cost** command. To reset the path cost to the default, use the **no** form of this command.

ospfv3 cost *interface-cost*

no ospfv3 cost *interface-cost*

Syntax Description

<i>interface-cost</i>	Unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Defaults

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

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 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 **auto-cost** 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 Enterprise Services license.

Examples

This example shows how to configure the interface cost value to 65:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 cost 65
```

Related Commands

Command	Description
auto-cost (OSPFv3)	Specifies the reference bandwidth that OSPFv3 uses to calculate the link cost.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ospfv3 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 **ospfv3 dead-interval** command. To restore the default, use the **no** form of this command.

ospfv3 dead-interval *seconds*

no ospfv3 dead-interval

Syntax Description

<i>seconds</i>	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. The value must be the same for all nodes on the network.

Defaults

The default for *seconds* is four times the interval set by the **ospfv3 hello-interval** command.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 dead-interval** command to set the dead interval that OSPFv3 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 ospfv3 interface** command to verify the dead interval and hello interval.

This command requires the Enterprise Services license.

Examples

This example shows how to set the OSPFv3 dead interval to 20 seconds:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ospfv3 dead-interval 20
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ospfv3 hello-interval	Interval between hello packets that OSPFv3 sends on the interface.
show ospfv3 interface	Displays OSPFv3-related information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ospfv3 hello-interval

To specify the interval between hello packets that Open Shortest Path First version 3 (OSPFv3) sends on the interface, use the **ospfv3 hello-interval** command. To return to the default, use the **no** form of this command.

ospfv3 hello-interval *seconds*

no ospfv3 hello-interval

Syntax Description	<i>seconds</i> Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.					
Defaults	10 seconds					
Command Modes	Interface configuration					
SupportedUserRoles	network-admin vdc-admin					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(1)	This command was introduced.
Release	Modification					
4.0(1)	This command was introduced.					
Usage Guidelines	Use the ospfv3 hello-interval command to set the rate at which OSPFv3 advertises hello packets. Shorter hello intervals allow OSPFv3 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 Enterprise Services license.					
Examples	This example shows how to set the interval between hello packets to 15 seconds: <pre>switch(config)# interface ethernet 1/2 switch(config-if)# ospfv3 hello-interval 15</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ospfv3 dead-interval</td><td>Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.</td></tr></table>		Command	Description	ospfv3 dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.
Command	Description					
ospfv3 dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router as down.					

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ospfv3 mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on received Database Descriptor (DBD) packets, use the **ospfv3 mtu-ignore** command. To return to the default, use the **no** form of this command.

ospfv3 mtu-ignore

no ospfv3 mtu-ignore

Syntax Description	This command has no arguments or keywords.

Defaults	OSPFv3 MTU mismatch detection is enabled.

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ospfv3 mtu-ignore command to disable MTU mismatch detection on an interface. By default, OSPFv3 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, OSPFv3 does not establish adjacencies. Use the ospfv3 mtu-ignore command to disable this check and allow adjacencies when the MTU value differs between OSPFv3 neighbors.

This command requires the Enterprise 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)# ospfv3 mtu-ignore
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ospfv3 network

To configure the Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for an interface, use the **ospfv3 network** command. To return to the default, use the **no** form of this command.

ospfv3 network { broadcast | point-to-point }

no ospfv3 network

Syntax Description	broadcast	Sets the network type as broadcast.
	point-to-point	Sets the network type as point-to-point.

Defaults	Depends on the network type.

Command Modes	Interface configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	The network type influences the behavior of the OSPF interface. 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 requires the Enterprise Services license.

Examples	This example shows how to set an OSPFv3 network as a broadcast network:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 address 2001:0DB8::1/8
switch(config-if)# ospfv3 network broadcast
```

Send document comments to nexus7k-docfeedback@cisco.com

ospfv3 passive-interface

To suppress Open Shortest Path First version 3 (OSPFv3) routing updates on an interface, use the **ospfv3 passive-interface** command. To return to the default, use the **no** form of this command.

ospfv3 passive-interface

no ospfv3 passive-interface

Syntax Description	This command has no keywords or arguments.

Defaults	Disabled

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	If an interface is configured as passive-interface it does not participate in the OSPF protocol and will not establish adjacencies or send routing updates. However the interface is announced as part of the routing network.

This command requires the Enterprise Services license.

Examples	This example shows how to set an interface as passive:

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ospfv3 passive-interface
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ospfv3 priority

To set the router priority for an Open Shortest Path First version 3 (osPFv3) interface, use the **ospfv3 priority** command. To return to the default, use the **no** form of this command.

ospfv3 priority *number-value*

no ospfv3 priority *number-value*

Syntax Description	<i>number-value</i>	Number value that specifies the priority of the router. The range is from 0 to 255.

Defaults	Priority of 1

Command Modes	Interface configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ospfv3 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. This command requires the Enterprise Services license.

Examples	This example shows how to set the router priority value to 4: <pre>switch(config)# interface ethernet 1/2 switch(config-if)# ospfv3 priority 4</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ospfv3 network	Configures the OSPFv3 network type to a type other than the default for a given medium.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ospfv3 retransmit-interval

To specify the time between Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ospfv3 retransmit-interval** command. To return to the default, use the **no** form of this command.

ospfv3 retransmit-interval *seconds*

no ospfv3 retransmit-interval

Syntax Description	<i>seconds</i>	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.

Defaults	5 seconds

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ospfv3 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 Enterprise 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)# ospfv3 retransmit-interval 8
```

Send document comments to nexus7k-docfeedback@cisco.com

ospfv3 shutdown

To shut down an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 shutdown** command. To return to the default, use the **no** form of this command.

ospfv3 shutdown

no ospfv3 shutdown

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the ospfv3 shutdown command to shut down OSPFv3 on this interface. This command requires the Enterprise Services license.

Examples	This example shows how to shut down OSPFv3 on an interface: switch(config)# interface ethernet 1/2 switch(config-if)# ospfv3 shutdown

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

ospfv3 transmit-delay

To set the estimated time required to send an Open Shortest Path First version 3 (OSPFv3) link-state update packet on the interface, use the **ospfv3 transmit-delay** command. To return to the default, use the **no** form of this command.

ospfv3 transmit-delay *seconds*

no ospfv3 transmit-delay

Syntax Description

<i>seconds</i>	Time (in seconds) required to send a link-state update. The range is from 1 to 450 seconds.

Defaults

1 second

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ospfv3 transmit-delay** command to set the estimated time needed to send an LSA update packet. OSPFv3 increments the LSA age time by 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 Enterprise 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)# ospfv3 transmit-delay 8
```

Send document comments to nexus7k-docfeedback@cisco.com



P Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter P.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

platform ip verify

To configure IP packet verification, use the **platform ip verify** command. To return to default, use the **no** form of this command.

platform ip verify {checksum | fragment | tcp tiny-frag | version}

no platform ip verify {checksum | fragment}

Syntax Description

checksum	Drops IPv4 or IPv6 packets if the checksum is invalid
fragment	Drops IPv4 or IPv6 packets if the packet fragment has a nonzero offset and the DF bit is active.
tcp tiny-frag	Drops IPv4 packets if the IP fragment offset is 1, or if the IP fragment offset is 0 and the IP payload length is less than 16.
version	Drops IPv4 packets if the ethertype is not set to 4 (IPv4).

Defaults

All address tests enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(3)	This command was replaced by the hardware ip verify command.

Usage Guidelines

Use the **platform ip verify** command to configure packet verification tests on IPv4 and IPv6 packets based on checksum or fragments.

This command does not require a license.

Examples

This example shows how to drop fragmented IPv4 or IPv6 packets:

```
switch(config)# platform ip verify fragment
```

Related Commands

Command	Description
platform ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
platform ip verify length	Configures IPv4 packet verification checks based on length.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
platform ipv6 verify	Configures IPv6 packet verification.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

Send document comments to nexus7k-docfeedback@cisco.com

platform ip verify address

To packet verification on IP addresses, use the **platform ip verify address** command. To return to default, use the **no** form of this command.

platform ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}

no platform ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}

Syntax Description	
destination zero	Drops IP packets if the destination IPv4 address is 0.0.0.0 or if the IPv6 address is ::.
identical	Drops IP packets if the source IPv4 or IPv6 address is identical to the destination IPv4 or IPv6 address.
reserved	Drops IP packets if the IPv4 address is in the 127.x.x.x range or if the IPv6 address is in the ::1 range.
source	Drops IP packets based on the IP source address
broadcast	Drops IP packets if the IP source address is 255.255.255.255
multicast	Drops IP packets if the IPv4 source address is in the 224.x.x.x range or if the IPv6 source address is in the FF00::/8 range.

Defaults All address tests enabled.

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(3)	This command was replaced by the hardware ip verify address command.

Usage Guidelines Use the **platform ip verify address** command to configure packet verification tests on IPv4 and IPv6 packets based on addresses.

This command does not require a license.

Examples This example shows how to drop broadcast IPv4 packets:

```
switch(config)# platform ip verify address source broadcast
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	platform ip verify	Configures IPv4 and IPv6 packet verification checks based on checksum or fragments.
	platform ip verify length	Configures IPv4 packet verification checks based on length.
	platform ipv6 verify	Configures IPv6 packet verification.
	show hardware forwarding ip verify	Displays information about IP packet verification checks.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

platform ip verify length

To configure IPv4 packet verification based on packet length, use the **platform ip verify length** command. To return to default, use the **no** form of this command.

platform ip verify length {consistent | maximum {max-frag | max-tcp | udp} | minimum}

no platform ip verify length {consistent | maximum {max-frag | max-tcp | udp} | minimum}

Syntax Description

consistent	Drops IPv4 packets where the Ethernet frame size is greater than or equal to the IP packet length plus the Ethernet header.
maximum {max-frag max-tcp udp}	Drops IPv4 packets based on the following: max-frag—Drops IP packets if the maximum fragment offset is greater than 65536. max-tcp—Drops IP packets if the TCP length is greater than the IP payload length. udp—Drops IP packets if the IP payload length is less than the UDP packet length.
minimum	Drops IP packets if the Ethernet frame length is less than the IP packet length plus four octets (the CRC length).

Defaults

All address tests enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(3)	This command was replaced by the hardware ip verify length command.

Usage Guidelines

Use the **platform ip verify length** command to configure packet verification tests on IPv4 and IPv6 packets based on packet length.

This command does not require a license.

Examples

This example shows how to drop minimum-length IPv4 packets:

```
switch(config)# platform ip verify length minimum
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	platform ip verify	Configures IPv4 packet verification checks based on checksum or fragments.
	platform ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
	platform ipv6 verify	Configures IPv6 packet verification.
	show hardware forwarding ip verify	Displays information about IP packet verification checks.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

platform ipv6 verify

To configure IPv6 packet verification, use the **platform ipv6 verify** command. To return to default, use the **no** form of this command.

platform ipv6 verify {length {consistent | maximum {max-frag | max-tcp | udp} | tcp tiny-frag | version}

no platform ip verify {checksum | fragment}

Syntax Description

length	Drops IPv6 packets based on length.
consistent	Drops IPv6 packets where the Ethernet frame size is greater than or equal to the IPv6 packet length plus the Ethernet header.
maximum {max-frag max-tcp udp}	Drops IPv6 packets based on the following: max-frag—Drops IPv6 packets if the formula (IPv6 Payload Length – IPv6 Extension Header Bytes) + (Fragment Offset * 8) is greater than 65536. max-tcp—Drops IPv6 packets if the TCP length is greater than the IP payload length. udp—Drops IPv6 packets if the IP payload length is less than the UDP packet length.
tcp tiny-frag	Drops IPv6 packets if the IP fragment offset is 1, or if the IPv6 fragment offset is 0 and the IPv6 payload length is less than 16.
version	Drops IPv6 packets if the ethertype is not set to 6 (IPv6).

Defaults

All address tests enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(3)	This command was replaced by the hardware ipv6 verify command.

Usage Guidelines

Use the **platform ipv6 verify** command to configure packet verification tests on IPv6 packets. This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to drop all IPv4 packets:

```
switch(config)# platform ipv6 verify version
```

Related Commands

Command	Description
platform ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
platform ip verify length	Configures IPv4 packet verification checks based on length.
show hardware forwarding ip verify	Displays information about IP packet verification checks.

Send document comments to nexus7k-docfeedback@cisco.com

policy statistics enable (OSPF)

To enable Open Shortest Path First (OSPF) policy statistics, use the **policy statistics enable** command. To disable policy statistics, use the **no** form of this command.

policy statistics enable

no policy statistics enable

Syntax Description

This command has no keywords or arguments.

Defaults

Policy statistics are disabled.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **policy statistics enable** command to enable statistics gathering based on route policies applied to this OSPF instance.

This command requires the Enterprise Services license.

Examples

The following example shows how to enable policy statistics gathering on OSPF 2:

```
switch(config)# ospf 2  
switch(config-router)# policy statistics enable
```

Related Commands

Command	Description
show ip ospf policy statistics	Shows policy statistics.

Send document comments to nexus7k-docfeedback@cisco.com

policy statistics enable (OSPFv3)

To enable Open Shortest Path First version 3 (OSPFv3) policy statistics, use the **policy statistics enable** command. To disable policy statistics, use the **no** form of this command.

policy statistics enable

no policy statistics enable

Syntax Description	This command has no keywords or arguments.

Defaults	Policy statistics are disabled.

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the policy statistics enable command to enable statistics gathering based on route policies applied to this OSPFv3 instance. This command requires the Enterprise Services license.

Examples	This example shows how to enable policy statistics gathering on OSPFv3 2:

```
switch(config)# ospfv3 2  
switch(config-router)# policy statistics enable
```

Related Commands	Command	Description
	show ospfv3 policy statistics	Shows policy statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

preempt (GLBP)

To configure the gateway to take over as active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group if it has a higher priority than the current AVG, use the **glbp preempt** command. To disable this feature, use the **no** form of this command.

Cisco NX-OS Release 4.1(3) and later syntax:

preempt [**delay minimum** *seconds*]

no preempt [**delay minimum** *seconds*]

Cisco NX-OS Release 4.1(2) and earlier syntax:

preempt [**delay minimum** *seconds*]

no preempt [**delay minimum** *seconds* [**sync** *seconds*]]

Syntax Description	delay minimum <i>seconds</i>	(Optional) Specifies a minimum number of seconds that the gateway delays before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.
	sync <i>seconds</i>	(Optional) Specifies a number of seconds that the gateway waits for the synchronization to complete. The range is from 0 to 3600 seconds .

Defaults	A GLBP gateway with a higher priority than the current AVG cannot assume the role of AVG. The default delay value is 30 seconds.

Command Modes	GLBP configuration

SupportedUserRoles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.1(3)	Removed sync keyword.
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to configure a router to preempt the current AVG when its priority of 254 is higher than the current AVG. If the router preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

```
switch(config-if)# glbp 10
switch(config-glbp)# preempt delay minimum 60
switch(config-glbp)# priority 254
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
priority	Sets the priority level of the router within a GLBP group.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 <i>min-delay</i>	(Optional)	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 <i>rel-delay</i>	(Optional)	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 <i>seconds</i>	(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.

Defaults The default delay time for all options is 0 seconds.

Command Modes Interface configuration or HSRP template mode

Supported User Roles Network administrator
VDC administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

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. Note that 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, then it assumes there is no active router for the group and will become active as soon as possible.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure a delay when a router becomes active when its priority 110.

```
switch# configure terminal
switch(config)# interface ethernet 0/1
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
```

Related Commands

Command	Description
feature hsrp	Enables HSRP configuration.
show hsrp	Displays HSRP information.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults

Enabled

Command Modes

VRRP configuration mode

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modification
4.0(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, 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.

If the virtual IP address is also the IP address for the interface, then preemption is applied.

No license is required to use this command.

Examples

This example shows how to enable the backup high-priority virtual router to preempt the low-priority master virtual router:

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

This preemption does not apply to the primary IP address.

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# preempt
```

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.
clear vrrp	Clears all the software counters for the specified virtual router.

Send document comments to nexus7k-docfeedback@cisco.com

priority (GLBP)

To set the priority level of the gateway within a Gateway Load Balancing Protocol (GLBP) group, use the **priority** command. To remove the priority level of the gateway, use the **no** form of this command.

priority *level*

no priority

Syntax Description	<i>level</i>	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.

Defaults	<i>level</i> : 100

Command Modes	GLBP configuration

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the priority command to control which virtual gateway becomes the active virtual gateway (AVG). GLBP compares the priorities of all virtual gateways in the GLBP group and selects the gateway with the numerically highest priority as the AVG. If two virtual gateways have equal priority, GLBP selects the gateway with the highest IP address. This command does not require a license.

Examples	The following example shows how to configure a virtual gateway with a priority of 254:

```
switch(config-if)# glbp 10
switch(config-glbp)# priority 254
```

Related Commands	Command	Description
	glbp	Enters GLBP configuration mode and creates a GLBP group.
	preempt	Configures a gateway to take over as the AVG for a GLBP group if it has a higher priority than the current AVG.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>level</i>	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	Sets the threshold used by a virtual port channel (vPC) to determine when to fail over to the vPC trunk.
	lower <i>lower-value</i>	Sets the low threshold value. The <i>lower-value</i> range is from 1 to 255. The default is 1.
	upper <i>upper-value</i>	Sets the upper threshold value. The <i>upper-value</i> range is from 1 to 255. The default is 255.

Defaults	<i>level</i> : 100 <i>lower-value</i> : 1 <i>upper-value</i> : 255

Command Modes	HSRP configuration or HSRP template mode

Supported User Roles	Network administrator VDC administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(3)	Added support for forwarding-threshold , lower , and upper keywords.

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. This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

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)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 4
switch(config-if-hsrp)# priority 254
```

Related Commands

Command	Description
feature hsrp	Enables HSRP configuration.
show hsrp	Displays HSRP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>level</i>	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	Sets the threshold used by a virtual port channel (vPC) to determine when to fail over to the vPC trunk.
	lower <i>lower-value</i>	Sets the low threshold value. The <i>lower-value</i> range is from 1 to 255. The default is 1.
	upper <i>upper-value</i>	Sets the upper threshold value. The <i>upper-value</i> range is from 1 to 255. The default is 255.

Defaults The default value is 100. For switches whose interface IP address is the same as the primary virtual IP address, the default value is 255.

Command Modes VRRP configuration mode

Supported User Roles network-admin
VDC administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.2(1)	Added support for forwarding-threshold , lower , and upper keywords.

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 will function 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.

No license is required to use this command.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to specify the priority for a virtual router:

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# vrrp 250  
switch(config-if-vrrp)# priority 2
```

Related Commands

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults	The OSPF instance is enabled by default when configured.

Command Modes	Router configuration Router VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the protocol shutdown command to configure disable an instance of OSPF without removing the configuration. This command requires the Enterprise Services license.

Examples	The following example shows how to disable OSPF 209: switch(config) router ospf 209 switch(config-router)# protocol shutdown

Send document comments to nexus7k-docfeedback@cisco.com

protocol shutdown (OSPFv3)

To shut down an Open Shortest Path First version 3 (OSPFv3) 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 keywords or arguments.

Defaults

The OSPFv3 instance is enabled by default when configured.

Command Modes

Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **protocol shutdown** command to configure disable an instance of OSPFv3 without removing the configuration.

This command requires the Enterprise Services license.

Examples

This example shows how to disable OSPFv3 209:

```
switch(config) router ospfv3 209
switch(config-router) # protocol shutdown
```

Send document comments to nexus7k-docfeedback@cisco.com



R Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter R.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 | isis instance-tag | ospf instance-tag | rip instance-tag |
static} [route-map map-name]
```

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

Syntax Description

bgp <i>as-number</i>	Distributes routes from the BGP protocol. 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 <i>instance-tag</i>	Name of EIGRP instance. The instance-tag can be any case-sensitive alphanumeric string up to 20 characters.
isis <i>instance-tag</i>	Distributes routes from the IS-IS protocol. The instance-tag can be any case-sensitive alphanumeric string up to 64 characters.
ospf <i>instance-tag</i>	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 64 characters.
rip <i>instance-tag</i>	Distributes routes from the RIP protocol. The instance-tag can be any case-sensitive alphanumeric string up to 64 characters.
static	Redistributes IP static routes.
route-map <i>map-name</i>	(Optional) Specifies the identifier of a configured route map. Use a route map to filter which routes are redistributed into EIGRP.

Defaults

Disabled.

Command Modes

Address family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Added eigrp keyword.

Send document comments to nexus7k-docfeedback@cisco.com

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 Enterprise Services license.

Examples

The following example shows how to redistribute cause 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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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* | **isis** *instance-tag* | **ospf** *instance-tag* | **rip** *instance-tag* | **static** } [**route-map** *map-name*]

no redistribute { **bgp** *as-number* | **direct** | **eigrp** *as-number* | **isis** *instance-tag* | **ospf** *instance-tag* | **rip** *instance-tag* | **static** }

Syntax Description		
bgp <i>as-number</i>		Distributes routes from the BGP protocol. 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 <i>id</i>		Name of EIGRP instance. The instance-tag can be any case-sensitive alphanumeric string up to 20 characters.
isis <i>instance-tag</i>		Distributes routes from the IS-IS protocol.
ospf <i>instance-tag</i>		Distributes routes from the OSPF protocol. This protocol is supported in the IPv4 address family.
rip <i>instance-tag</i>		Distributes routes from the RIP protocol.
static		Redistributes IP static routes.
route-map <i>map-name</i>		(Optional) Specifies the identifier of a configured route map. Use a route map to filter which routes are redistributed into EIGRP.

Defaults Disabled.

Command Modes Address family configuration
Router configuration
Router VRF configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

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.

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 Enterprise Services license.

Examples

The following 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
```

The following example shows how to redistribute the specified IS-IS process routes into an EIGRP autonomous system within a virtual routing and forwarding instance (VRF). The IS-IS routes are redistributed using route map IsIsMap.

```
switch(config)# router eigrp 109  
switch(config-router)# vrf Red  
switch(config-router-vrf)# redistribute isis 108 route-map IsIsMap
```

Related Commands

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

redistribute (IS-IS)

To redistribute other protocol routes into Intermediate System-to-Intermediate System (IS-IS), use the **redistribute** configuration mode command. To disable the redistribution, use the **no** form of this command.

redistribute *protocol as-num[.as-num] | process-tag route-map name*

no redistribute *protocol as-num[.as-num] | process-tag route-map name*

Syntax Description

<i>protocol</i>	Source protocol from which routes are being redistributed; see the “Usage Guidelines” section for additional information about valid values.
<i>as-num</i>	AS number. Range: 1 to 65535
<i>.as-num</i>	(Optional) AS number. Range: 0 to 65535
<i>process-tag</i>	Process tag.
route-map name	Prevents distribution of a specific route map.

Command Default

Cisco NX-OS software does not redistribute routes.

Command Modes

Address family configuration
Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The command syntax is supported for IPv4 and IPv6.

The valid values for the *protocol* argument are as follows:

- **bgp as-num[.as-num] route-map name**—Specifies the route map for the Border Gateway Protocol (BGP) routes. Range: 1 to 65535. Range: 0 to 65535 for the optional *as-num* argument.
- **direct route-map name**—Specifies the route map for the directly connected routes.
- **eigrp process-tag route-map name**—Specifies the route map for the Enhanced Interior Gateway Protocol (EIGRP) routes.
- **isis process-tag route-map name**—Specifies the route map for the ISO IS-IS routes.
- **ospf process-tag route-map name**—Specifies the route map for the Open Shortest Path First (OSPF) routes.

Send document comments to nexus7k-docfeedback@cisco.com

- **rip *process-tag* route-map *name***—Specifies the route map for the Routing Information Protocol (RIP) routes for IPv4.
- **static route-map *name***—Specifies the route map for the static routes.

Examples

The following example shows how to redistribute routes from an IS-IS routing process into a BGP system:

```
switch(config)# router isis firstcompany  
switch(config-router)# redistribute bgp 34535 route-map test1
```

The following example shows how to disable redistribution:

```
switch(config)# router isis firstcompany  
switch(config-router)# no redistribute bgp 34535 route-map test1
```

Related Commands

Command	Description
address-family	Enters the address family mode or a VRF address-family mode.
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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* | **isis** *instance-tag* | **ospf** *instance-tag* | **rip** *instance-tag* | **static** } [**route-map** *map-name*]

no redistribute { **bgp** *as-number* | **direct** | **eigrp** *as-number* | **isis** *instance-tag* | **ospf** *instance-tag* | **rip** *instance-tag* | **static** }

Syntax Description

bgp <i>as-number</i>	(Optional) Distributes routes from the BGP protocol. The <i>as-number</i> 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 <i>id</i>	Distributes routes from EIGRP. The <i>instance-tag</i> argument can be any case-sensitive alphanumeric string.
isis <i>instance-tag</i>	Distributes routes from the IS-IS protocol. The <i>instance-tag</i> argument can be any case-sensitive alphanumeric string.
ospf <i>instance-tag</i>	Distributes routes from the OSPF protocol. This protocol is supported in the IPv4 address family. The <i>instance-tag</i> argument can be any case-sensitive alphanumeric string.
static	Redistributes IP static routes, including the default static route.
route-map <i>map-name</i>	(Optional) Specifies the identifier of a configured route map. Use a route map to filter which routes are redistributed into EIGRP. The <i>route-map</i> argument can be any alphanumeric string.

Defaults

Route redistribution is disabled.

Command Modes

Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Changed the eigrp keyword to use a process tag.

Send document comments to nexus7k-docfeedback@cisco.com

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.

You need to 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 Enterprise Services license.

Examples

The following example shows how to redistribute BGP routes into an OSPF autonomous system:

```
switch(config)# router ospf 209  
switch(config-router)# redistribute bgp 64496
```

The following example shows how to redistribute the specified IS-IS process routes into an OSPF autonomous system within a virtual routing and forwarding instance (VRF). The IS-IS routes are redistributed using route map IsIsMap.

```
switch(config)# router ospf 109  
switch(config-router)# vrf Red  
switch(config-router-vrf)# redistribute isis 108 route-map IsIsMap
```

Related Commands

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

redistribute (OSPFv3)

To inject routes from one routing domain into Open Shortest Path First version 3 (OSPFv3), 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 | isis instance-tag | rip instance-tag | static} [route-map
map-name]
```

```
no redistribute {bgp as-number | direct | eigrp as-number | isis instance-tag | ospfv3 instance-tag
| rip instance-tag | static}
```

Syntax Description

bgp <i>as-number</i>	(Optional) Distributes routes from the BGP protocol. 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 <i>id</i>	Distributes routes from EIGRP. The <i>instance-tag</i> argument can be any case-sensitive alphanumeric string.
isis <i>instance-tag</i>	Distributes routes from the IS-IS protocol. The <i>instance-tag</i> argument can be any case-sensitive alphanumeric string.
static	Redistributes IP static routes, including the default static route.
route-map <i>map-name</i>	(Optional) Specifies the identifier of a configured route map. Use a route map to filter which routes are redistributed into EIGRP. The <i>route-map</i> argument can be any alphanumeric string.

Defaults

Route redistribution is disabled.

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Changed the eigrp keyword to use a process tag.

Usage Guidelines

Use the **redistribute** command to import routes from other routing protocols into OSPFv3. You should always use a route map to filter these routes to ensure that OSPFv3 redistributes only the routes that you intend.

Send document comments to nexus7k-docfeedback@cisco.com

You need to configure a default metric to redistribute routes from another protocol into OSPFv3. 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 Enterprise Services license.

Examples

This example shows how to redistribute BGP routes into an OSPFv3 autonomous system:

```
switch(config)# router ospfv3 209  
switch(config-router)# address-family ipv6 unicast  
switch(config-router-af)# redistribute bgp 64496
```

Related Commands

Command	Description
default-metric (OSPFv3)	Sets the default metrics for routes redistributed into OSPFv3.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

redistribute (RIP)

To redistribute routes from another routing domain into the Routing Information Protocol (RIP), use the **redistribute** command in the router address-family configuration mode. 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* | **isis** *id* | **ospf** *id* | **ospfv3** *id* | **static** } **route-map** *map-name*

Syntax Description

bgp	Redistributes routes from the Border Gateway Protocol (BGP).
direct	Redistributes routes from directly connected routes only.
eigrp	Redistributes routes from the Enhanced Interior Gateway Routing Protocol (EIGRP).
isis	Redistributes routes from the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
ospf	Redistributes routes from the Open Shortest Path First (OSPF) protocol.
ospfv3	Redistributes routes from the Open Shortest Path First version 3 (OSPFv3) protocol.
static	Redistributes routes from IP static routes.
<i>id</i>	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 decimal number, but Cisco NX-OS stores it internally as a string. For the isis keyword, an IS-IS instance name from which routes are to be redistributed. The value takes the form of a string. You can enter decimal number, but Cisco NX-OS 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. A decimal number can be entered, but it is stored internally as a string.
route-map <i>map-name</i>	Associates a route map to set the redistribution policy for RIP.

Defaults

Route redistribution is disabled.

Command Modes

Router address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Cisco NX-OS 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 NX-OS determines the metric based on the redistributed protocol or by the **default-metric** command. If Cisco NX-OS cannot determine a valid metric, then it does not redistribute the routes.

This command does not require a license.

Examples

The following 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
```

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

redistribute maximum-prefix

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

<i>max</i>	maximum number of prefixes that OSPF will distribute. The range is from 0 to 65536.
<i>threshold</i>	(Optional) Percent of maximum prefixes that will trigger a warning message. The range is from 1 to 100. The default is 75%.
warning-only	(Optional) Logs an warning message when the maximum number of prefixes is exceeded.
withdraw	(Optional) Withdraws all redistributed routes.
<i>num-retries</i>	(Optional) Number of times OSPF will try to retrieve the redistributed routes. The range is from 1 to 12. The default is 1.
<i>timeout</i>	(Optional) The time between retry attempts. The range is from 60 to 600 seconds. The default is 300.

Command Default

No limit

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **redistribute maximum-prefix** command to limit the number of routes redistributed into OSPF. Use the **clear ip ospf redistribute** command if all routes are withdrawn.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to limit the number of redistributed routes into OSPF:

```
switch# config t
switch(config)# router ospfv3 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# redistribute maximum-prefix 1000 75
```

Related Commands

Command	Description
feature ospf	Enables the OSPF feature.
feature ospfv3	Enables the OSPFv3 feature.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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		
<i>max</i>		maximum number of prefixes that EIGRP will distribute. The range is from 0 to 65536.
<i>threshold</i>		(Optional) Percent of maximum prefixes that will trigger a warning message. The range is from 1 to 100. The default is 75%.
warning-only		(Optional) Logs an warning message when the maximum number of prefixes is exceeded.
withdraw		(Optional) Withdraws all redistributed routes.
<i>num-retries</i>		(Optional) Number of times EIGRP will try to retrieve the redistributed routes. The range is from 1 to 12. The default is 1.
<i>timeout</i>		(Optional) The time between retry attempts. The range is from 60 to 600 seconds. The default is 300.

Command Default No limit

Command Modes Router configuration
VRF configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines Use the **redistribute maximum-prefix** command to limit the number of routes redistributed into EIGRP. Use the **clear ip eigrp redistribute** command if all routes are withdrawn.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to limit the number of redistributed routes into EIGRP:

```
switch# config t
switch(config)# router eigrp 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# redistribute maximum-prefix 1000 75
```

Related Commands

Command	Description
feature eigrp	Enables the EIGRP feature.
redistribute (EIGRP)	Configures route redistribution for EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

redistribute maximum-prefix (IS-IS)

To limit the number of routes redistributed into Intermediate System to Intermediate System (IS-IS), 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	
<i>max</i>	maximum number of prefixes that IS-IS will distribute. The range is from 0 to 65536.
<i>threshold</i>	(Optional) Percent of maximum prefixes that will trigger a warning message. The range is from 1 to 100. The default is 75%.
warning-only	(Optional) Logs an warning message when the maximum number of prefixes is exceeded.
withdraw	(Optional) Withdraws all redistributed routes.
<i>num-retries</i>	(Optional) Number of times IS-IS will try to retrieve the redistributed routes. The range is from 1 to 12. The default is 1.
<i>timeout</i>	(Optional) The time between retry attempts. The range is from 60 to 600 seconds. The default is 300.

Command Default No limit

Command Modes Router configuration
VRF configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines Use the **redistribute maximum-prefix** command to limit the number of routes redistributed into IS-IS. Use the **clear isis redistribute** command if all routes are withdrawn.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to limit the number of redistributed routes into IS-IS:

```
switch# config t
switch(config)# router isis 201
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# redistribute bgp route-map FilterExternalBGP
switch(config-router-af)# redistribute maximum-prefix 1000 75
```

Related Commands

Command	Description
feature isis	Enables the IS-IS feature.
redistribute (IS-IS)	Configures route redistribution for IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

reference-bandwidth

To change the reference bandwidth used to assign the IS-IS cost, use the **reference-bandwidth** command. To return to the default setting, use the no form of this command.

reference-bandwidth { *gbps* | *mbps* } [*gbps* | **mbps**]

no reference-bandwidth

Syntax Description

<i>gbps</i>	Reference bandwidth in gigabits per second (gbps). Range: 1 to 4000. Default: 40.
<i>mbps</i>	Reference bandwidth in megabits per second (mbps). Range: 1 to 4000000. Default: 40000.
gbps	(Optional) Specifies Gbps.
mbps	(Optional) Specifies Mbps.
route-map <i>name</i>	Prevents distribution of a specific route map.

Command Default

Bandwidth is in Mbps.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If you do not enter the **gbps** or the **mbps** keyword, Mbps is the default.

The cost of interfaces is calculated by comparing the interface bandwidth with a reference bandwidth. The **reference-bandwidth** command configures the reference bandwidth.

Examples

The following example shows how to set the reference bandwidth to 3500 Gbps:

```
switch(config)# router isis firstcompany
switch(config-router)# reference-bandwidth 3500 gbps
```

The following example shows how to return to the default reference bandwidth:

```
switch(config)# router isis firstcompany
switch(config-router)# no reference-bandwidth
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>number</i>	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.

Defaults	None

Command Modes	neighbor configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to configure the neighbor AS number: <pre>switch(config)# router bgp 64496 switch(config-router)# neighbor 10.0.0.100 switch(config-router-neighbor)#remote-as 64497</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

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

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>seconds</i>	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.

Defaults	5 seconds

Command Modes	Virtual link configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the retransmit-interval 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 Enterprise Services license.

Examples	The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

retransmit-interval (OSPFv3 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	<i>seconds</i>	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.

Defaults	5 seconds

Command Modes	Virtual link configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the retransmit-interval 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 Enterprise Services license.

Examples	This example shows how to set the retransmit interval value to 8 seconds: <pre>switch(config)# router ospfv3 109 switch(config-router)# area 33 virtual-link 192.0.2.2 switch(config-router-vrf)# retransmit-interval 8</pre>

Related Commands	Command	Description
	area virtual-link	Creates a virtual link in an OSPFv3 area.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 in global configuration mode. 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

<i>map-tag</i>	Route map name.
deny	(Optional) Specifies that the route or packet is not distributed as follows: - If the match criteria are met for the route map, the route is not redistributed. - With policy routing, the packet is not policy routed and route maps sharing the same map tag name are not examined. If the packet is not policy routed, the normal forwarding algorithm is used.
permit	(Optional) Specifies that the route or packet is distributed as follows: - If the match criteria for this route are met, the route is redistributed as controlled by the set actions. With policy routing, the packet is policy routed. - If the match criteria are not met, the next route map with the same map tag is tested. If a route does not pass any of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.
<i>sequence-number</i>	(Optional) Number that indicates the position a new route map will have 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

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enter the **feature pbr** global configuration mode command to enable PBR before entering the **route-map** command.

Send document comments to nexus7k-docfeedback@cisco.com

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)#
```

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 expires 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.
 - **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 route. See the **match ip next-hop** command for additional information.
 - route-source**—Matches the advertising source address of route. See the **match ip route-source** command for additional information.
 - **ipv6**—Configures the IPv6 features. The follow keywords and arguments are available:
 - address** {*access-list-name* [*access-list-name*] | **prefix-list** *ipv6-list-name* [*ipv6-list-name*]}—Specifies the address of the route or packet to match. See the **match ipv6 address prefix-list** command for additional information.



Note The IPv6 access-list name is for use in route-maps for PBR only.

multicast {**group** *address/length* | **rp** *address/length*}—Specifies the multicast attributes to match. See the **match ipv6 multicast** command for additional information.

next-hop prefix-list—Matches the next-hop address of route. See the **match ipv6 next-hop prefix-list** command for additional information.

route-source—Matches the advertising source address of route. See the **match ipv6 route-source prefix-list** command for additional information.

Send document comments to nexus7k-docfeedback@cisco.com

- **length** *minimum-length maximum-length*—Defines the minimum and maximum packet length. See the **match length** command for additional information.
- **route-type**—Matches the route-type of the route. See the **match route-type** command for additional information.
- **tag**—Matches the metric of route. See the **match tag** command for additional information.



Note

The **default-information originate** command ignores **match** statements in the optional route map.

- **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.
 - **ip**—Configures the IP features. The following keywords and arguments are available:
 - set ip default next-hop**—Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination. See the **set ip default next-hop** command for additional information.
 - set ip next-hop**—Indicates where to output packets that pass a match clause of a route map for policy routing. See the **set ip next-hop** command for additional information.
 - **ipv6**—Configures the IPv6 features. The following keywords and arguments are available:
 - set ipv6 default next-hop**—Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination. See the **set ipv6 default next-hop** command for additional information.
 - set ipv6 next-hop**—Indicates where to output packets that pass a match clause of a route map for policy routing. See the **set ipv6 next-hop** 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 destination routing protocol. See the **set metric** command for additional information.
 - **metric-type**—Sets the type of metric for destination routing protocol. See the **set metric-type** command for additional information.

Send document comments to nexus7k-docfeedback@cisco.com

- **origin**—Specifies the BGP origin code. See the **set origin** command for additional information.
- **tag**—Specifies the tag value for destination routing protocol. See the **set tag** command for additional information.
- **vrf**—Sets the VRF for next-hop resolution. See the **set vrf** 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 or to subject packets to policy routing. Both purposes are described in this section.

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 relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Policy Routing

Use the **ip policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. 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 guidelines for the *sequence-number* argument are as follows:

1. If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
2. If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number* argument of this entry is unchanged.
3. If more than one entry is defined with the supplied tag, an error message is printed to indicate that the *sequence-number* argument is required.

Send document comments to nexus7k-docfeedback@cisco.com

If the **no route-map map-tag** command is specified (with no *sequence-number* argument), the whole route map is deleted.

Examples

The following example redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes will be 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
```

The following example for IPv6 redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes will be redistributed into OSPF as external link-state advertisements (LSAs) with a tag equal to 42 and a metric type equal to type1.

```
switch(config)# router 1
switch(config-route-map)# redistribute rip one route-map ripng-to-ospfv3
switch(config)# route-map ripng-to-ospfv3
switch(config-route-map)# match tag 42
switch(config-route-map)# set metric-type type1
```

The following 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
```

The following example shows that the routes matching community list 1 will have the weight set to 100. Any route that has community 109 will have 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
```

The following example shows that the routes matching community list 1 will have the weight set to 200. Any route that has community 109 alone will have 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
switch(config-route-map)# set weight 200
```

In the following example, the routes that match community list LIST_NAME will have the weight set to 100. Any route that has community 101 alone will have 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

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

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, and performs policy routing on packets.
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, or enables policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

route-map pbr-statistics

To enable policy-based statistics for a route map, use the **route-map pbr statistics** command. To disable statistics, use the **no** form of this command.

route-map *name* **pbr-statistics**

no route-map *name* **pbr-statistics**

Syntax Description

<i>name</i>	Name of the route map. The name can be any alphanumeric string up to 63 characters.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **route-map pbr-statistics** command to enable policy-based routing statistics. You must enable policy-based routing with the **feature pbr** command before you can enable policy-based routing statistics.



Note

This command may fail if the same interface is configured for some other policy such as ACLs.

This command requires the Enterprise Services license.

Examples

This example shows how to enable the policy-base routing statistics for a route map:

```
switch(config)# feature pbr
switch(config)# route-map testmap pbr-statistics
```

Related Commands

Command	Description
clear route-map pbr-statistics	Clears policy-based routing statistics for a route map.

Send document comments to nexus7k-docfeedback@cisco.com

router bgp

To enter the assign an autonomous system (AS) number to a router and enter the router BGP configuration mode, use the **router bgp** command in global configuration mode. 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	<i>as-num</i>	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.
	<i>.as-num</i>	(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.

Defaults No BGP routing process is enabled by default.

Command Modes Address-family configuration
Neighbor address-family configuration
Router BGP configuration

SupportedUserRoles network-admin
vdc-admin

Usage Guidelines 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 bestpath 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.

Send document comments to nexus7k-docfeedback@cisco.com

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 is a single autonomous system.

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 mismatch of AS numbers, the peer is sent an error code update notification message. To disable, 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 link goes down. Only directly connected peering sessions are supported.

If BGP fast external fallover is disabled, the BGP routing process will wait until the default hold timer expires (three keepalives) to reset the peering session.

- **graceful-restart**—Configures the Graceful Restart functionality (router, vrf). See the **graceful-restart (BGP)** command for additional information.
- **graceful-restart-helper**—Configures the Graceful Restart Helper mode functionality (router, vrf). See the **graceful-restart (BGP)** command for additional information.
- **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 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** and **show bgp ipv6 neighbors** commands.

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.

Send document comments to nexus7k-docfeedback@cisco.com

- **no**—Negates a command or set 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**—Configure the BGP-related timers (router, vrf).
 - **bestpath-limit interval**—Configures timeout for first bestpath after restart in seconds. Range: 1 to 3600. Default: 300.
 - **bgp interval**—Configures the different BGP keepalive and holdtimes in seconds. Range: 0 to 3600. Default: 60.
 - **prefix-peer-timeout interval**—Configures how long state for 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.

Examples

The following example configures a BGP process for autonomous system 120:

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

The following example logs neighbor changes for BGP in router configuration mode:

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

In the following example, the BGP fast external fallover feature is disabled. If the link through which this session is carried flaps, the connection will not be reset.

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

In the following example, 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. In the follow example, updates from the 10.100.0.1 peer will be 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)#
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	Name of EIGRP instance. The instance-tag can be any case-sensitive alphanumeric string up to 20 characters.

Defaults

None

Command Modes

Global

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

router isis

To configure a routing process and enter router configuration mode for Intermediate System to Intermediate System (IS-IS), use the **router isis** command. To turn off the IS-IS routing process, use the **no** form of this command.

router isis *instance-tag*

no router isis *instance-tag*

Syntax Description	<i>instance-tag</i> Instance name. The name can be any alphanumeric string up to 20 characters.	
Defaults	None	
Command Modes	Global	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command requires the Enterprise Services license.	
Examples	The following example shows how to configure a routing process for IS-IS: switch(config)# router isis test1 switch(config-router)#	
Related Commands	Command	Description
	default-information	Controls the distribution of a default route.
	distance	Configures the administrative distance.
	maximum-paths	Configures the maximum number of equal-cost paths.
	redistribute	Configures route redistribution for IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>instance-tag</i>	Internally used identification parameter for an OSPF routing instance. It is locally assigned and can be any word or positive integer. The <i>instance-tag</i> argument can be any alphanumeric string.

Defaults	No OSPF routing instance is defined.

Command Modes	Global configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	This example shows how to configure a basic OSPF instance: switch(config)# router ospf 12

Send document comments to nexus7k-docfeedback@cisco.com

router ospfv3

To configure an Open Shortest Path First version 3 (OSPFv3) routing instance, use the **router ospfv3** command. To terminate an OSPFv3 routing process, use the **no** form of this command.

router ospfv3 *instance-tag*

no router ospfv3 *instance-tag*

Syntax Description	<i>instance-tag</i>	Internally used identification parameter for an OSPFv3 routing instance. It is locally assigned and can be any word or positive integer. The <i>instance-tag</i> argument can be any alphanumeric string.
Defaults	No OSPFv3 routing instance is defined.	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Use the router ospfv3 command to specify multiple OSPFv3 routing instances in each router. This command requires the Enterprise Services license.	
Examples	This example shows how to configure a basic OSPFv3 instance: switch(config)# router ospfv3 12	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

router rip

To configure the the Routing Information Protocol (RIP) routing process, use the **router rip** command in global configuration mode. To turn off the RIP routing process, use the **no** form of this command.

router rip *instance-tag*

no router rip

Syntax Description

<i>instance-tag</i>	Name for this RIP instance.

Command Default

No RIP routing process is defined.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

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

<i>router-id</i>	32-bit router ID value specified in four-part, dotted-decimal notation.

Defaults

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
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

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

<i>ip-address</i>	Router ID in IP address format.

Defaults

If this command is not configured, OSPF chooses an IPv4 address as the router ID from one of its interfaces.

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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.

Send document comments to nexus7k-docfeedback@cisco.com

router-id (OSPFv3)

To use a fixed router ID for an Open Shortest Path First version 3 (OSPFv3) instance, use the **router-id** command. To revert to the previous OSPFv3 router ID behavior, use the **no** form of this command.

router-id *ip-address*

no router-id *ip-address*

Syntax Description	<i>ip-address</i> Router ID in IP address format.	
Defaults	If this command is not configured, OSPFv3 chooses an IPv4 address as the router ID from one of its interfaces.	
Command Modes	Router configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 OSPFv3 instance that has neighbors, OSPFv3 uses the new router ID at the next reload or at a restart of OSPFv3. This command requires the Enterprise Services license.	
Examples	This example shows how to configure the router ID: <pre>switch(config)# router ospfv3 12 switch(config-router)# router-id 192.0.2.1</pre>	
Related Commands	Command	Description
	router ospfv3	Configures the OSPFv3 routing process.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

routing-context vrf

To set the virtual routing and forwarding (VRF) scope for all EXEC commands, use the **routing-context vrf** command. To revert to default behavior, use the **no** form of this command.

routing-context vrf *vrf-name*

no routing-context vrf *vrf-name*

Syntax Description	<i>vrf-name</i>	Name of the VRF instance. The name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	default VRF.

Command Modes	EXEC

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 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. This command does not require a license.

Examples	This example shows how to limit EXEC commands to the management VRF: <pre>switch# routing-context vrf management switch%management#</pre>

Related Commands	Command	Description
	show routing-context	Displays the current routing context.



S Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter S, except for the **show** commands.

set as-path

To modify an autonomous system path (as-path) for BGP routes, use the **set as-path** command in route-map configuration mode. 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 BGP.
	prepend <i>as-num</i>	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 one AS number.
	last-as <i>num</i>	Prepends the last AS numbers to the as-path. Range: 1 to 10.

Defaults	Autonomous system path is not modified.

Command Modes	Route-map configuration (config-route-map)

Supported User Roles	network-admin vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enter the **feature pbr** global configuration mode command to enable PBR before entering the **route-map** 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 **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

The following example converts the tag of a redistributed route into an autonomous system path:

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

The following example prepends 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
!

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 address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
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, or enables policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set comm-list delete

To remove communities from the community attribute of an inbound or outbound update, use the **set comm-list delete** command in route-map configuration mode. 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

<i>community-list-name</i>	A 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 (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 will be 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**).

Send document comments to nexus7k-docfeedback@cisco.com

This command does not require a license.

Examples

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

```
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 address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
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, or enables policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

set community

To set the BGP communities attribute, use the **set community** route map configuration 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	<i>aa:nn</i>	(Optional) 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 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	(Optional) Adds to existing community. You can configure one or more keywords.
	local-AS	(Optional) 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 external peers or to other subautonomous systems within a confederation. You can configure one or more keywords.
	no-advertise	(Optional) 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	(Optional) 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.
	none	(Optional) Specifies the no community attribute. You cannot configure any other keyword if you configure the none keyword.

Command Default No BGP communities attributes exist.

Command Modes Route-map configuration (config-route-map)

Supported User Roles network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(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.

This command does not require a license.

Examples

In the following example, routes that pass the autonomous system path access list 1 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 will not be 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
```

In the following similar example, routes that pass the autonomous system path access list 1 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 will 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, or enables policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set dampening

To set the BGP route dampening factors, use the **set dampening** route map configuration 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		
	<i>half-life</i>	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. Range: 1 to 45. Default: 15.
	<i>reuse</i>	Unsuppresses the route 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.
	<i>suppress</i>	Suppresses a route when its penalty exceeds this limit. Range: 1 to 20000. Default: 2000.
	<i>max-suppress-time</i>	Maximum time (in minutes) a route can be suppressed. Range: 1 to 255. Default: Four times the <i>half-life</i> value. If the <i>half-life</i> value is allowed to default, the maximum suppress time defaults to 60 minutes.

Command Default	This command is disabled by default.

Command Modes	Route-map configuration (config-route-map)

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 <i>match criteria</i>—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the <i>set actions</i>—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.

Send document comments to nexus7k-docfeedback@cisco.com

This command does not require a license.

Examples

The following 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
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 address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
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, or enables policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

set etxcommunity

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

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

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

Syntax Description	
none	(Optional) 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.
<i>aa4:nn</i>	(Optional) 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	(Optional) Adds to existing community.

Command Default No BGP communities attributes exist.

Command Modes Route-map configuration (config-route-map)

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines Use the **set etxcommunity** 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.

Send document comments to nexus7k-docfeedback@cisco.com

This command does not require a license.

Examples

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

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.
match extcommunity	Matches an extended community in a route map.
ip extcommunity-list	Creates a community list for BGP and controls access to it.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>community-list-name</i>	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 (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **set extcomm-list** 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*).

This command does not require a license.

Examples

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

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

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

set forwarding-address

To set the OSPF forwarding address for redistributed type-5 LSAs, use the **set forwarding-address** route-map configuration mode 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 (config-route-map)

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command is used by the Open Shortest Path First (OSPF) to set the forwarding address in the 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 non-zero. The 0.0.0.0 address indicates that the originating router (the ASBR) is the next hop. The forwarding address is determined by these conditions: The forwarding address is set to 0.0.0.0 if the ASBR redistributes routes and OSPF is not enabled on the next hop interface for those routes. This is true in the figure if Router 1 does not have OSPF enabled on the Ethernet interface.

All of the following conditions must be met to set the forwarding address field to a non-zero 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.

Any other conditions besides those listed previously, set the forwarding address to 0.0.0.0.

This command does not require a license.

Examples	The following example shows how to set the forwarding address:

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

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config-route-map)# set forwarding-address
```

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, and performs policy routing on packets.
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, or enables policy routing.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set ip default next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination, use the **set ip default next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ip default next-hop *ip-address* [...*ip-address*] [**load-share**]

no set ip default next-hop *ip-address* [...*ip-address*]

Syntax Description	<i>ip-address</i>	IP address of the next hop to which packets are output. The next hop must be an adjacent router. You can configure up to 32 IP addresses.
	load-share	(Optional) Enables load sharing.

Command Default	This command is disabled by default.

Command Modes	Route-map configuration (config-route-map)

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the <i>ip-address</i> argument.

Use this command to provide certain users a different default route. If the software has no explicit route for the destination in the packet, then it routes the packet to this next hop. The first next hop specified with the **set ip default next-hop** command needs to be adjacent to the router. The optional specified IP addresses are tried in turn.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. 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 policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

Send document comments to nexus7k-docfeedback@cisco.com

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set ip default next-hop**



Note

The **set ip next-hop** and **set ip default next-hop** are similar commands but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ip default next-hop** command causes the system to use the routing table first and then policy route the specified next hop.

This command does not require a license.

Examples

The following example shows how to configure a route map that sets the IPv6 default next-hop address.

```
switch(config)# ip access-list test
switch(config-ip-acl)# permit ip 192.0.2.0/24 any
switch(config-ip-acl)# exit
switch(config)# route-map equal-access
switch(config-route-map)# match ip address test
switch(config-route-map)# set ip default next-hop ip 192.0.2.3
switch(config-route-map)# exit
switch(config)# interface externet 2/1
switch(config-if)# ip policy route-map equal-access
```

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, and performs policy routing on packets.
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, or enables policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

```
set ip next-hop {ip-address [... ip-address] [load-share] | peer-address}
```

```
no set ip next-hop {ip-address [... ip-address] [load-share] | peer-address}
```

Syntax Description

<i>ip-address</i>	IP address of the next hop to which packets are output. It need not be an adjacent router. You can configure one or more IP addresses.
load-share	(Optional) Enables load sharing.
peer-address	Sets the next hop to be the BGP peering address.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. 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 policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

When the **set ip next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

Send document comments to nexus7k-docfeedback@cisco.com

When the **set ip next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ip next-hop** command has finer granularity than the (per-neighbor) **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set ip default next-hop**

This command does not require a license.

Examples

In the following example, three routers are on the same LAN (with IP addresses 10.1.1.1, 10.1.1.2, and 10.1.1.3). Each is in a different autonomous system. The **set ip next-hop peer-address** command specifies that traffic from the router (10.1.1.3) in remote autonomous system 64496 for the router (10.1.1.1) in remote autonomous system 64497 that matches the route map is passed through the router bgp 64498, rather than sent directly to the router (10.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```
switch(config)# router bgp 64498
switch(config-router)# neighbor 10.1.1.3 remote-as 64496
switch(config-router)# neighbor 10.1.1.3 route-map set-peer-address out
switch(config-router)# neighbor 10.1.1.1 remote-as 64497
!
switch(config)# route-map set-peer-address permit 10
switch(config-route-map)# set ip next-hop peer-address
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set ipv6 default next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination, use the **set ipv6 default next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 default next-hop *ipv6-address* [...*ipv6-address*] [**load-share**]

no set ipv6 default next-hop *ipv6-address* [...*ipv6-address*]

Syntax Description

<i>ipv6-address</i>	IPv6 address of the next hop to which packets are output. The next hop must be an adjacent router. You can configure up to 32 IPv6 addresses.
load-share	(Optional) Enables load sharing.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ipv6-address* argument.

Use this command to provide certain users a different default route. If the software has no explicit route for the destination in the packet, then it routes the packet to this next hop. The first next hop specified with the **set ipv6 default next-hop** command needs to be adjacent to the router. The optional specified IP addresses are tried in turn.

Use the **ipv6 policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ipv6 policy route-map** command identifies a route map by name. 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 policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

Send document comments to nexus7k-docfeedback@cisco.com

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set ipv6 default next-hop**



Note

The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands but have a different order of operations. Configuring the **set ipv6 next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ipv6 default next-hop** command causes the system to use the routing table first and then policy route the specified next hop.

This command does not require a license.

Examples

The following example shows how to configure a route map that sets the IPv6 default next-hop address.

```
switch(config)# ipv6 access-list test
switch(config-ipv6-acl)# permit ipv6 2001:0DB8::/48 any
switch(config-ipv6-acl)# exit
switch(config)# route-map equal-access
switch(config-route-map)# match ipv6 address test
switch(config-route-map)# set ipv6 default next-hop 2001:0DB8::3
switch(config-route-map)# exit
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 policy route-map equal-access
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
match ipv6 next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ipv6 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, or enables policy routing.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set ipv6 next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

```
sset ipv6 next-hop {ipv6-address [... ipv6-address] [load-share] | peer-address}
```

```
no set ipv6 next-hop {ipv6-address [... ipv6-address] [load-share] | peer-address}
```

Syntax Description

<i>ipv6-address</i>	IPv6 address of the next hop to which packets are output. It need not be an adjacent router. You can configure one or more IP addresses.
load-share	(Optional) Enables load sharing.
peer-address	Sets the next hop to be the BGP peering address.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ipv6-address* argument.

Use this command to provide certain users a different default route. If the software has no explicit route for the destination in the packet, then it routes the packet to this next hop. The first next hop specified with the **set ipv6 default next-hop** command needs to be adjacent to the router. The optional specified IP addresses are tried in turn.

Use the **ipv6 policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ipv6 policy route-map** command identifies a route map by name. 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 policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

Send document comments to nexus7k-docfeedback@cisco.com

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set ipv6 default next-hop**



Note

The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands but have a different order of operations. Configuring the **set ipv6 next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ipv6 default next-hop** command causes the system to use the routing table first and then policy route the specified next hop.

This command does not require a license.

Examples

The following example shows how to configure a route map that sets the IPv6 next-hop address.

```
switch(config)# ipv6 access-list test
switch(config-ipv6-acl)# permit ipv6 2001:0DB8::/48 any
switch(config-ipv6-acl)# exit
switch(config)# route-map equal-access
switch(config-route-map)# match ipv6 address test
switch(config-route-map)# set ipv6 next-hop 2001:0DB8::3
switch(config-route-map)# exit
switch(config)# interface externet 2/1
switch(config-if)# ipv6 policy route-map equal-access
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
match ipv6 next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ipv6 route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set ipv6 default next-hop	Specifies the address of the next hop.

Send document comments to nexus7k-docfeedback@cisco.com

set level

To indicate where to import routes, use the **set level** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

```
set level {level-1 | level-2 | level-1-2}
```

```
no set level {level-1 | level-2 | level-1-2}
```

Syntax Description	level-1	Imports routes into a Level 1 area.
	level-2	Imports routes into a Level 2 subdomain.
	level-1-2	Imports routes into Level 1 and Level 2.

Command Default	This command is disabled by default.

Command Modes	Route-map configuration (config-route-map)

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

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.

This command does not require a license.

Examples	In the following example, routes will be imported into the Level 1 area:

```
switch(config-router)# route-map testcase
switch(config-route-map)# set level level-1
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
neighbor next-hop-self	Disables next hop processing of BGP updates on the router.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco NX-OS software has no explicit route to a destination.

Send document comments to nexus7k-docfeedback@cisco.com

set local-preference

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

set local-preference *number-value*

no set local-preference *number-value*

Syntax Description	<i>number-value</i> Preference value. Range: 0 to 4294967295. Default: 100.	
Command Default	Preference value of 100 by default.	
Command Modes	Route-map configuration (config-route-map)	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 <i>match criteria</i>—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the <i>set actions</i>—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 <i>set actions</i> 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. This command does not require a license.	
Examples	The following example sets the local preference to 100 for all routes that are included in access list 1: <pre>switch(config-router)# route-map map-preference switch(config-route-map)# match as-path 1 switch(config-route-map)# set local-preference 100</pre>	

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	match as-path	Matches a BGP autonomous system path access list.
	match community	Matches a BGP community.
	match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
	match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
	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 (IP)	Redistributes routes with the metric specified.
	match route-type (IP)	Redistributes routes of the specified type.
	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, or enables policy routing.
	set automatic-tag	Automatically computes the tag value.
	set community	Sets the BGP communities attribute.
	set ip next-hop	Specifies the address of the next hop.
	set level (IP)	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 (IP)	Sets the value of the destination routing protocol.

Send document comments to nexus7k-docfeedback@cisco.com

set metric

To set the metric value for a routing protocol, use the **set metric** command in route-map configuration mode. 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.
<i>bandwidth-metric</i>	Interior Gateway Routing Protocol (IGRP) bandwidth metric, in Kb/s. The range is from 0 to 4294967295..
<i>delay-metric</i>	(Optional) Interior Gateway Routing Protocol (IGRP) delay metric, in 10 microsecond units. The range is from 1 to 4294967295.
<i>reliability-metric</i>	(Optional) IGRP reliability metric. The range is from 0 to 255.
<i>load-metric</i>	(Optional) IGRP load metric. The range is from 1 to 255.
<i>mtu</i>	(Optional) IGRP maximum transmission unit (MTU) of the path. The range is from 1 to 4294967295.

Command Default None

Command Modes Route-map configuration (config-route-map)

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added the + and - keywords.

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 configure the *reliability-metric* and the *load-metric* arguments, 255 means 100 percent reliability.

Send document comments to nexus7k-docfeedback@cisco.com

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 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.

This command does not require a license.

Examples

The following example shows how to set the bandwidth metric value for the routing protocol to 100:

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

The following example shows how to increase the bandwidth metric value for the routing protocol by 100:

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

Related Commands

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

Send document comments to nexus7k-docfeedback@cisco.com

set metric-type

To set the metric type for the destination routing protocol, use the **set metric-type** command in route-map configuration mode. To return to the default, use the **no** form of this command.

set metric-type {internal | external | type-1 | type-2}

no set metric-type {internal | external | type-1 | type-2}

Syntax Description	internal	Specifies the Intermediate System-to-Intermediate System (IS-IS) internal metric, or the Interior Gateway Protocol (IGP) metric as the multi-exit discriminator (MED) for BGP.
	external	Specifies the IS-IS external metric.
	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 (config-route-map)

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

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).

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example sets the metric type of the destination protocol to OSPF external Type 1:

```
switch(config)# route-map map-type
switch(config-route-map)# set metric-type 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 address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.
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, or enables policy routing.
set as-path	Sets a BGP autonomous system path access list.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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 origin	Sets the BGP origin code.
set tag	Sets the value of the destination routing protocol.

Send document comments to nexus7k-docfeedback@cisco.com

set origin

To set the BGP origin code, use the **set origin** route-map configuration mode 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 <i>as-num</i> [: <i>as-num</i>]	Specifies the 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 (config-route-map)

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example sets the origin of routes that pass the route map to IGP:

```
switch(config)# route-map set_origin
switch(config-route-map)# match as-path 10
switch(config-route-map)# set origin igp
```

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, and performs policy routing on packets.
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, or enables policy routing.
set as-path	Sets a BGP autonomous system path access list.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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 origin	Sets the BGP origin code.
set tag	Sets the value of the destination routing protocol.

Send document comments to nexus7k-docfeedback@cisco.com

set tag

To set a tag value of the destination routing protocol, use the **set tag** command in route-map configuration mode. To delete the entry, use the **no** form of this command.

set tag *tag-value*

no set tag *tag-value*

Syntax Description	<i>tag-value</i> Name for the tag. Integer from 0 to 4294967295.	
Command Default	If not specified, the default action is to <i>forward</i> the tag in the source routing protocol onto the new destination protocol.	
Command Modes	Route-map configuration (config-route-map)	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 <i>match criteria</i>—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the <i>set actions</i>—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 <i>set actions</i> 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. This command does not require a license.	
Examples	The following example sets the tag value of the destination routing protocol to 5: <pre>switch(config)# route-map test switch(config-route-map)# set tag 5</pre>	

Send document comments to nexus7k-docfeedback@cisco.com

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, and performs policy routing on packets.
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, or enables policy routing.
set as-path	Sets a BGP autonomous system path access list.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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 origin	Sets the BGP origin code.
set tag	Sets the value of the destination routing protocol.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set vrf

To enable virtual routing/forwarding instance (VRF) selection within a route map for policy-based routing VRF selection, use the **set vrf** command in route-map configuration mode. To disable VRF selection within a route map, use the **no** form of this command.

set vrf { *vrf-name* | **default** | **management** }

no set vrf [*vrf-name* | **default** | **management**]

Syntax Description

<i>vrf-name</i>	Name assigned to the VRF.
default	Sets the VRF to the default VRF.
management	Sets the VRF to the management VRF.

Command Default

No default behavior or values

Command Modes

Route-map configuration (config-route-map)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **set vrf** route-map configuration command was introduced with the MPLS VPN—VRF Selection using Policy Based Routing feature to provide a PBR mechanism for VRF selection. This command is used to enable VRF selection by policy routing packets through a route map. The route map is attached to the incoming interface. Match criteria is defined in an IP access list or in an IP prefix list. Match criteria can also be defined based on packet length with the **match length** route map command. The VRF must be defined prior to the configuration of this command, and the **ip policy route-map** interface configuration command must be configured to enable policy routing under the interface or subinterface. If the VRF is not defined or if policy routing is not enabled, an error message will be printed in the console when you attempt to configure the **set vrf** command.



Note

The **set vrf** command cannot be configured with the **set ip default next-hop**, and **set ip next-hop** policy routing commands because a packet cannot be set to an interface and the next hop cannot be changed when the VRF is specified. This is designed behavior. An error message will be printed in the console if you attempt to configure the **set vrf** command with any of the four above set clauses.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows a route-map sequence that selects and sets a VRF based on match criteria defined in three different access lists. (The access list configuration is not shown in this example.) If the route map falls through and a match does not occur, the packet will be dropped if the destination is local.

```
switch(config)# route-map PBR-VRF-Selection permit 10
switch(config-route-map)# match ip address 40
switch(config-route-map)# set vrf VRF_1
!
switch(config)# route-map PBR-VRF-Selection permit 20
switch(config-route-map)# match ip address 50
switch(config-route-map)# set vrf VRF_2
!
switch(config)# route-map PBR-VRF-Selection permit 30
switch(config-route-map)# match ip address 60
switch(config-route-map)# set vrf VRF_3
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
debug ip policy	Displays IP policy routing packet activity.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ip vrf	Configures a VRF routing table.
ip vrf receive	Inserts the IP address of an interface as a connected route entry in a VRF routing table.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, or performs policy routing on packets.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

Send document comments to nexus7k-docfeedback@cisco.com

set weight

To specify the BGP weight for the routing table, use the **set weight** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set weight *number*

no set weight [*number*]

Syntax Description	<i>number</i> Weight value. Range: 0 to 65535.								
Defaults	The weight is not changed by the specified route map.								
Command Modes	Route-map configuration (config-route-map)								
Supported User Roles	network-admin vdc-admin								
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.				
Release	Modification								
4.0(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. In other words, the weights assigned with the set weight route-map configuration command override the weights assigned using the neighbor weight command. This command does not require a license.								
Examples	The following example sets the BGP weight for the routes matching the autonomous system path access list to 200: <pre>switch(config)# route-map set-weight switch(config-route-map)# match as-path 10 switch(config-route-map)# set weight 200</pre>								
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>match as-path</td><td>Matches a BGP autonomous system path access list.</td></tr><tr><td>match community</td><td>Matches a BGP community.</td></tr><tr><td>match ip address</td><td>Distributes any routes that have a destination network number address that is permitted by a standard or expanded access list, and performs policy routing on packets.</td></tr></table>	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, and performs policy routing on packets.
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, and performs policy routing on packets.								

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
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, or enables policy routing.
set as-path	Sets a BGP autonomous system path access list.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
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 origin	Sets the BGP origin code.
set tag	Sets the value of the destination routing protocol.

Send document comments to nexus7k-docfeedback@cisco.com

set-attached-bit

To set the attached (ATT) bit for Intermediate-System-to-Intermediate System (IS-IS), use the **set-attached-bit** command. To disable this function, use the **no** form of this command.

set-attached-bit

no set-attached-bit

Syntax Description	This command has no keywords or arguments.

Defaults	Enabled

Command Modes	Router configuration VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	Use set-attached-bit command to configure whether to use a Level 1/Level 2 IS-IS router as the default router for Level 1 routers in the same area. If the set-attached-bit command is disabled, the "attached-bit" will not be advertised by the router in its Level 1 LSP, and other Level 1 routers in the area will not use this router as the default router outside the area.

This command requires the Enterprise Services license.

Examples	The following example shows how to unset the attached bit:

```
switch(config)# router isis Border1  
switch(config-router)# no set-attached-bit
```

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

set-overload-bit

To configure the router to signal other routers not to use this router as an intermediate hop in their shortest path first (SPF) calculations, use the **set-overload-bit** command. To remove the designation, use the **no** form of this command.

```
set-overload-bit {always | {on-startup {seconds | wait-for bgp as-num[.as-num]}} [suppress
[[interlevel] [external]]]
```

```
no set-overload-bit
```

Syntax Description		
always		Sets the overload bit unconditionally.
on-startup <i>seconds</i>		Sets the overload bit at system startup. The overload bit remains set for the number of seconds configured. Range: 5 to 86400.
on-startup wait-for bgp		Causes the overload bit to be set upon system startup and remains set until BGP has converged.
<i>as-num</i>		AS number. Range: 1 to 65535
<i>.as-num</i>		(Optional) AS number. Range: 0 to 65535
suppress		(Optional) Causes the type of prefix identified by the subsequent keyword or keywords to be suppressed.
interlevel		(Optional) Prevents the IP prefixes that are learned from another IS-IS level from being advertised.
external		(Optional) Prevents the IP prefixes that are learned from other protocols from being advertised.

Command Default The overload bit is not set by default.

Command Modes Router configuration
VRF configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines The **set-overload-bit** command forces the router to set the overload bit in its nonpseudonode link-state packets (LSPs). Normally, the setting of the overload bit is allowed only when a router runs into problems. For example, when a router is experiencing a memory shortage, it might be that the link-state

Send document comments to nexus7k-docfeedback@cisco.com

database is not complete, resulting in an incomplete or inaccurate routing table. By setting the overload bit in its LSPs, other routers can ignore the unreliable router in their SPF calculations until the router has recovered from its problems.

The results are that no paths through this router are seen by other routers in the IS-IS area. However, IP and Connectionless Network Service (CLNS) prefixes directly connected to this router are reachable.

This command can be useful when you want to connect a router to an IS-IS network but do not want real traffic flowing through it under any circumstances. Examples situations are as follows:

- A test router in the lab, connected to a production network.
- A router configured as an LSP flooding server, for example, on a nonbroadcast multiaccess (NBMA) network, in combination with the mesh group feature.
- A router that is aggregating virtual circuits (VCs) used only for network management. In this case, the network management stations must be on a network directly connected to the router with the set-overload-bit command configured.

Unless you specify the **on-startup** keyword, this command sets the overload bit immediately.

In addition to setting the overload bit, you might want to suppress certain types of IP prefix advertisements from LSPs. For example, allowing IP prefix propagation between level 1 and level 2 effectively makes a node a transit node for IP traffic, which might be undesirable. The suppress keyword used with the interlevel or external keyword (or both) accomplishes that suppression while the overload bit is set.

This command does not require a license.

Examples

The following example sets the overload bit upon startup and until BGP has converged:

```
switch(config)# router isis firstcompany
switch(config-router)# set-overload-bit on-startup wait for-bgp suppress interlevel external
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults

Enabled

Command Modes

Router configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **shutdown** command to disable an instance of BGP without removing the configuration. This command requires the Enterprise Services license.

Examples

The following example shows how to disable BGP 64496:

```
switch(config)# router BGP 64496
switch(config-router)# shutdown
```

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

Defaults	Enabled

Command Modes	Address family configuration Router configuration Router VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following example shows how to disable eigrp 209:

```
switch(config)# router eigrp 209  
switch(config-router)# shutdown
```

Send document comments to nexus7k-docfeedback@cisco.com

shutdown (IS-IS)

To stop an IS-IS router process without removing the process configuration, use the **shutdown** command. To start a stopped IS-IS process, 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
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following example stops an active IS-IS process:

```
switch(config)# router isis firstcompany
switch(config-router)# shutdown
```

The following example starts a stopped a IS-IS process:

```
switch(config)# router isis firstcompany
switch(config-router)# no shutdown
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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 VRF configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	This example stops 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.

Send document comments to nexus7k-docfeedback@cisco.com

shutdown (OSPFv3)

To stop an Open Shortest Path First (OSPFv3) 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
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

This example stops an active OSPFv3 instance:

```
switch(config)# router ospfv3 firstcompany
switch(config-router)# shutdown
```

Related Commands

Command	Description
feature ospfv3	Enables OSPFv3 on the router.
router ospv3f	Configures an OSPF v3 instance.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Defaults	Disabled

Command Modes	VRRP configuration mode

Supported User Roles	network-admin VDC administrator

Command History	Release	Modified
	4.0(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 administrative shut down state. Enter the no shutdown command to update the virtual router state after completing configuration. This command does not require a license.

Examples	This example shows how to shut down a VRRP group:

```
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
```

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.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

spf-interval

To configure the minimum interval between arrivals of a link-state advertisement (LSA), use the **spf-interval** command. To return to the default setting, use the **no** form of this command.

spf-interval [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait* *spf-second-wait*]

no spf-interval

Syntax Description	level-1	Specifies the shortest path first (SPF) level-1 interval.
	level-2	Specifies the SPF level-2 interval.
	<i>spf-max-wait</i>	Maximum interval (in milliseconds) between two consecutive SPF calculations. Range: 500 to 65535.
	<i>spf-initial-wait</i>	Initial SPF calculation delay (in milliseconds) after a topology change. Range: 50 to 65535.
	<i>spf-second-wait</i>	Hold time between the first and second SPF calculation (in milliseconds). Range: 50 to 65535.
Command Default	None	
Command Modes	Router configuration VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	An LSA is used to advertise connected networks. This command requires the Enterprise Services license.	

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to set the minimum interval time between arrivals of a LSA:

```
switch(config)# router isis firstcompany  
switch(config-router)# spf-interval level-1 500 500 500
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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 <i>map-name</i>	(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 Router configuration Router VRF configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 the EIGRP Stub Routing feature to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP will 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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

The following example shows how to configure the router as a receive-only neighbor:

```
switch(config)# router eigrp 1  
switch(config-router)# stub receive-only
```


Send document comments to nexus7k-docfeedback@cisco.com

summary-address

To create the IS-IS aggregate addresses, use the **summary-address** command. To remove the aggregate address, use the **no** form of this command.

summary-address {*ip-addr* | *ip-prefix/length* | *ipv6-addr* | *ipv6-prefix/length*} *level*

Syntax Description	<i>ip-addr</i>	IP address of the neighbor in this format: A.B.C.D.
	<i>ip-prefix/length</i>	IP prefix and the length of the IP prefix. The length of the IPv6 prefix is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. Use this format: A.B.C.D/length.
	<i>ipv6-addr</i>	IPv6 address of the neighbor in this format: A:B::C:D.
	<i>ipv6-prefix/length</i>	IPv6 prefix and the length of the IPv6 prefix for neighbors in this format: A:B::C:D/length.
	<i>level</i>	Level number. Default: All routes are advertised individually. Valid values are as follows: • level-1—Summarizes the IP address into the level-1 area. Only routes redistributed into level 1 are summarized with the configured address and mask value. • level-1-2—Summarizes the IP address into the level-1 and level-2 areas. Summary routes are applied when redistributing routes into level-1 and level-2 IS-IS, and when level-2 IS-IS advertises level-1 routes as reachable in its area. • level-2—Summarizes the IP address into the level-2 area. Routes learned by level-1 routing are summarized into the level-2 backbone with the configured address and mask value. Redistributed routes into level-2 IS-IS will be summarized also.
Command Default	None	
Command Modes	Address-family configuration Router configuration VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps network stability because a summary advertisement is depending on many more specific routes. A single route flap does not cause the summary advertisement to flap in most cases.

Note that when using summary addresses, other routes might have less information to calculate the most optimal routing table for all individual destinations are used.

This command requires the Enterprise Services license.

Examples

The following example redistributes directly connected routes into IS-IS. This example advertises only 10.1.0.0 into the IS-IS level-1 link-state protocol data unit (PDU). The summary address is tagged with 100.

```
switch(config)# router isis 100  
switch(config-router)# address-family ipv4 unicast  
switch(config-router-af)# redistribute direct route-map CORE1  
switch(config-router-af)# summary-address 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
address-family	Enters the address family mode or a VRF address-family mode.
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>ip-prefix/length</i>	IP prefix designated for a range of addresses, including the prefix length. Specify <i>ip-prefix</i> as an IP address. Specify <i>length</i> as a number from 1 to 31.
	not-advertise	(Optional) Suppress routes that match the specified prefix/length pair.
	tag <i>tag</i>	(Optional) Tag value that can be used as a “match” value for controlling redistribution using route maps. The range is from 1 to 65535.

Defaults	None

Command Modes	Router configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	redistribute (OSPF	Redistributes external routing protocol routes into OSPF.

Send document comments to nexus7k-docfeedback@cisco.com

summary-address (OSPFv3)

To create aggregate addresses for the Open Shortest Path First version 3 (OSPFv3) protocol, use the **summary-address** command. To return to the default, use the **no** form of this command.

summary-address *ipv6-prefix/length* [**not-advertise**] [**tag** *tag*]

no summary-address *ipv6-prefix/length* [**not-advertise**] [**tag** *tag*]

Syntax Description	<i>ipv6-prefix/length</i>	IP prefix designated for a range of addresses, including the prefix length. Specify <i>ip-prefix</i> as an IPv6 address. Specify <i>length</i> as a number from 1 to 128.
	not-advertise	(Optional) Suppress routes that match the specified prefix/length pair.
	tag <i>tag</i>	(Optional) Tag value that can be used as a “match” value for controlling redistribution using route maps. The range is from 1 to 65535.

Defaults	None

Command Modes	Address-family configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 OSPFv3 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 Enterprise 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 ospfv3 201
switch(config-router)# address-family ipv6 unicast
```

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config-router)# summary-address 2001:0DB8::0/16
```

Related Commands

Command	Description
redistribute (OSPFv3	Redistributes external routing protocol routes into OSPFv3.

Send document comments to nexus7k-docfeedback@cisco.com

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 keywords or arguments.

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

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 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(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
```

Related Commands

Command	Description
route-map <i>map-name</i>	Creates a route map.

 suppress-inactive

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com



Show Commands

This chapter describes the Cisco NX-OS unicast routing **show** commands.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show bgp

To display Border Gateway Protocol routes, use the **show bgp** command.

```
show bgp [{ipv4 | ipv6}] {unicast | multicast} | all [addr | prefix [longer-prefixes]] [vrf
vrf-name]
```

Syntax Description

ipv4	(Optional) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv4 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display BGP information for all address families.
<i>addr</i>	(Optional) A network from the selected address family. The format is A.B.C.D for IPv4 and A:B::C:D for IPv6.
<i>prefix</i>	Optional) A prefix from the selected address family. The format is A.B.C.D/length for IPv4 and A:B::C:D/length for IPv6.
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 63 characters.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added support for IPv6 addresses and prefixes.

Usage Guidelines

Use the **show bgp** command to display information about BGP. This command does not require a license.

Examples

This example displays an entry in the BGP table:

```
switch(config-router)# show bgp ipv6 unicast
BGP routing table information for VRF default, address family IPv6 Unicast
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	clear bgp	Clears entries in the BGP table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show bgp community

To display Border Gateway Protocol (BGP) routes that match a community, use the **show bgp community** command.

```
show bgp { { ipv4 | ipv6 } { unicast | multicast } | all } community [as-number] [internet]
[no-advertise] [no-export] [no-export-subconfed] [exact-match] } [vrf vrf-name]
```

Syntax Description	
ipv4	(Optional) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv6 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display BGP information for all address families.
<i>as-number</i>	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>.
internet	(Optional) Displays the internet community.
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.

Defaults None

Command Modes Any command mode

Supported User Roles

- network-admin
- network-operator
- vdc-admin
- vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example displays routes that match a community:

```
switch(config)# show bgp ip unicast community
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip community-list	Creates a community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 {{ipv4 | ipv6} {unicast | multicast} | all} community-list commlist-name
[exact-match] [vrf vrf-name]
```

Syntax Description	
ipv4	(Optional) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv6 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display BGP information for all address families.
<i>commlist-name</i>	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 <i>vrf-name</i>	(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

Supported User Roles

- network-admin
- network-operator
- vdc-admin
- vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example displays routes that match a community list:

```
switch(config)# show bgp ip unicast community-list test1
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
ip community-list	Creates a community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show bgp extcommunity

To display Border Gateway Protocol (BGP) routes that match an extended community, use the **show bgp extcommunity** command.

```
show bgp { { ipv4 | ipv6 } { unicast | multicast } | all } extcommunity generic { non-transitive |
transitive } [as4-number] [exact-match] [vrf vrf-name]
```

Syntax Description	
ipv4	(Optional) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv6 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display BGP information for all address families.
generic	Displays the routes that match the generic specific extended communities.
non-transitive	Displays the routes that match the non-transitive extended communities.
transitive	Displays the routes that match the transitive extended communities.
<i>as4-number</i>	AS number. The <i>as4-number</i> 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.

Defaults None

Command Modes Any command mode

Supported User Roles

- network-admin
- network-operator
- vdc-admin
- vdc-operator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example displays routes that match an extended community:

```
switch(config)# show bgp ip unicast xtcommunity generic transitive 1.3:30
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 {{ipv4 | ipv6} {unicast | multicast} | all} extcommunity-list commlist-name
[exact-match] [vrf vrf-name]
```

Syntax Description	
ipv4	(Optional) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv4 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display BGP information for all address families.
<i>commlist-name</i>	Name of an extended community-list. The <i>commlist-name</i> 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 63 characters.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a community list: <pre>switch(config)# show bgp ipv6 unicast extcommunity-list test1</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show bgp neighbors

To display Border Gateway Protocol (BGP) neighbors, use the **show bgp neighbors** command.

```
show bgp {ip | ipv6} {unicast | multicast} neighbors [addr [advertised-routes | flap-statistics |
paths | received-routes | routes [advertised | dampened | received]] | prefix] [vrf {all |
vrf-name}]
```

Syntax Description

<i>addr</i>	IPv4 address. The format is x.x.x.x
ip	Displays the IPv4 neighbor information.
ipv6	Displays the IPv6 neighbor information.
unicast	Displays the unicast neighbor information.
multicast	Displays the multicast neighbor information.
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.
<i>prefix</i>	(Optional) IPv6 prefix. The format is x.x.x.x/length.
vrf <i>vrf-name</i>	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
all	(Optional) Specifies all VRFS.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Added paths keyword.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines This command does not require a license.

Examples This example displays the BGP neighbors:

```
switch(config)# show bgp ip unicast neighbors
```

Related Commands	Command	Description
	show ip bgp neighbors	Displays the IPv4 BGP information.
	show ipv6 bgp neighbors	Displays the IPv6 BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show bgp sessions

To display Border Gateway Protocol (BGP) sessions, use the **show bgp sessions** command.

show bgp sessions [**vrf** *vrf-name*]

Syntax Description	<i>vrf vrf-name</i> (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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays BGP sessions: <pre>switch# show bgp sessions Total peers 0, established peers 0 ASN 33.33 VRF default, local ASN 33.33 peers 0, established peers 0, local router-id 192.168.1.222 State: I-Idle, A-Active, O-Open, E-Established, C-Closing, S-Shutdown Flaps LastUpDn LastRead LastWrit St Port(L/R) Notif(S/R)</pre>	
Related Commands	Command	Description
	clear bgp	Clears BGP sessions.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show forwarding

To display forwarding information, use the **show forwarding** command.

```
show forwarding [ip | ipv4 | ipv6] {adjacency | interfaces | route | trace [clear] | table id pss
route} [module slot] [vrf vrf-name]
```

Syntax Description	
ip	(Optional) Displays the IPv4 forwarding information.
ipv4	(Optional) Displays the IPv4 forwarding information.
ipv6	(Optional) Displays the IPv6 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 <i>id</i> range is from 0 to 2147483647.
pss route	Displays route information from persistent storage.
module slot	(Optional) Displays information for the module. The slot range depends on the hardware platform.
vrf vrf-name	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Modes	Any

Supported User Roles	network-adminr vdc-adminr

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added the trace and clear keywords.
	4.2(1)	Added the table pss route keywords.

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.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to display forwarding information for module 2:

```
switch# show forwarding route module 2
```

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

Related Commands

Command	Description
show ip fib	Displays information about the FIB.

Send document comments to nexus7k-docfeedback@cisco.com

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 FIB.

Command Modes	Any

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples This example displays forwarding information for unicast clients:

```
switch# show forwarding distribution clients
```

id	pid	shmem-start	shmem-end	shmem-name
1	3646	0x64f70120	0x64fc0000	u6rib-ufdm
2	3647	0x64b50120	0x64d50000	urib-ufdm

Related Commands	Command	Description
	show ip fib distribution	Displays distribution information about the FIB.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show forwarding inconsistency

To display the results of the forwarding inconsistency checker, use the **show forwarding inconsistency** command.

show forwarding inconsistency [**ip** | **ipv4** | **ipv6**] [**unicast**] **module** *slot* [**vrf** *vrf-name*]

Syntax Description	
ip	(Optional) Displays the IPv4 forwarding inconsistency information.
ipv4	(Optional) Displays the IPv4 forwarding inconsistency information.
ipv6	(Optional) Displays the IPv6 forwarding inconsistency information.
unicast	(Optional) Displays the forwarding inconsistency information for unicast routes
module <i>slot</i>	Displays inconsistency information for the module. The slot range depends on the hardware platform.
vrf <i>vrf-name</i>	(Optional) Displays inconsistency information for the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Modes Any

Supported User Roles Network Administrator
VDC Administrator

Command History	Release	Modification
	4.0(3)	This command was introduced.
	4.2(1)	Added support for ipv6 keyword.

Usage Guidelines Use the **show forwarding inconsistency** command to display the results of the **test forwarding inconsistency** command.

This command does not require a license.

Examples This example displays forwarding inconsistency information for module 2:

```
switch# show forwarding inconsistency module 2
Consistency check : table_id(0x1) slot(2)
No inconsistent adjacencies.
No inconsistent routes.
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	clear forwarding inconsistency	Clears the forwarding inconsistency checker.
	test forwarding inconsistency	Triggers the forwarding inconsistency checker.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command.

show glbp [**interface** *type number*] [**group** *number*] [*state*] [**brief**] [**vrf** *vrf-name*]

Syntax Description	interface <i>type number</i>	(Optional) Specifies the interface to display GLBP information.
	group <i>number</i>	(Optional) Specifies the GLBP group number. The range is from 0 to 1023.
	<i>state</i>	(Optional) State of the GLBP router. The states are as follows: active , disabled , init , listen , or standby .
	brief	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names. Supported in Cisco NX-OS Release 4.0(2) and later releases.

Command Modes	Any

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	Added support for vrf keyword.

Usage Guidelines	Use the show glbp command to display information about GLBP groups. The brief keyword displays a single line of information about each virtual gateway or virtual forwarder. This command does not require a license.

Examples	The following example shows how to display GLBP information:

```
switch# show glbp
```

```
Ethernet2/1 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 192.0.2.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
```

Send document comments to nexus7k-docfeedback@cisco.com

```

Authentication MD5, key "ThisStringIsTheSecretKey"
Preemption enabled, min delay 60 sec
Active is local
Standby is unknown
Priority 254 (configured)
Weighting 105 (configured 110), thresholds: lower 95, upper 105
  Track object 2 state Down decrement 5
Load balancing: host-dependent
Group members:
  0016.C76C.85DC (7.199.10.1) local
There is 1 forwarder (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 23:50:15
  MAC address is 0007.b400.0101 (default)
  Owner ID is 0005.0050.6c08
  Redirection enabled
  Preemption enabled, min delay 60 sec
  Active is local, weighting 105

```

The following example shows how to display a brief summary of GLBP information:

```
switch# show glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Eth2/1	10	-	254	Active	192.0.2.10	local	unknown
Eth1/2	10	1	7	Active	0007.b400.0101	local	-

The following example shows how to specify the GLBP interface and group number:

```
switch# show glbp interface ethernet2/2 group 1
```

```

Ethernet2/2 - Group 1
State is Listen
  64 state changes, last state change 00:00:54
Virtual IP address is 10.1.0.7
Hello time 50 msec, hold time 200 msec
  Next hello sent in 0.030 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Authentication text "authword"
Preemption enabled, min delay 0 sec
Active is 10.1.0.2, priority 105 (expires in 0.184 sec)
Standby is 10.1.0.3, priority 100 (expires in 0.176 sec)
Priority 96 (configured)
Weighting 100 (configured 100), thresholds: lower 95, upper 100
  Track object 1 state Up decrement 10
Load balancing: round-robin
Group members:
  0004.4d83.4801 (10.0.0.0)
  0010.7b5a.fa41 (10.0.0.1)
  00d0.bbd3.bc21 (10.0.0.2) local

```

Table 1-1 describes the significant fields shown in the displays.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Table 1-1 *show glbp Field Descriptions*

Field	Description
Ethernet2/1 - Group	Interface type and number and GLBP group number for the interface.
State is	State of the virtual gateway. For a virtual gateway, the state can be one of the following: • Active—The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. • Disabled—The virtual IP address has not been configured or learned yet, but another GLBP configuration exists. • Initial—The virtual IP address has been configured or learned, but the virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured. • Listen—The virtual gateway is receiving hello packets and is ready to change to the Speak state if the active or standby virtual gateway becomes unavailable. • Speak—The virtual gateway is attempting to become the active or standby virtual gateway. • Standby—The gateway is next in line to be the AVG. For a virtual forwarder, the state can be one of the following: • Active—The gateway is the active virtual forwarder (AVF) and is responsible for forwarding packets sent to the virtual forwarder MAC address. • Disabled—The virtual MAC address has not been assigned or learned. This state is transitory because a virtual forwarder that changes to a disabled state is deleted. • Initial—The virtual MAC address is known, but the virtual forwarder configuration is not complete. An interface must be up and configured to route IP, an interface IP address must be configured, and the virtual IP address must be known. • Listen—The virtual forwarder is receiving hello packets and is ready to change to the Active state if the AVF becomes unavailable.
Virtual IP address is	Virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If a virtual IP address is a duplicate of an address configured for another device, it will be marked as a duplicate. A duplicate address indicates that the router has failed to defend its ARP cache entry.
Hello time, hold time	Time between hello packets, in seconds or milliseconds, that indicates the hello time. The hold time is the time (in seconds or milliseconds) before other routers declare the active router to be down. All routers in a GLBP group use the hello-time and hold-time values of the current AVG. If the locally configured values are different, the configured values appear in parentheses after the hello-time and hold-time values.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-1 ***show glbp Field Descriptions (continued)***

Field	Description
Redirect time, forwarder time-out	Redirect and timeout times for an AVF transition to a standby virtual forwarder. The redirect time is the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF. The timeout is the time (in seconds) before the secondary virtual forwarder becomes unavailable.
Preemption	Whether GLBP gateway preemption is enabled. If enabled, the minimum delay is the time, in seconds, for which a higher-priority nonactive router will wait before preempting the lower-priority active router. This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.
Active is	Active state of the virtual gateway. The value can be local, unknown, or an IP address. The address (and the expiration date of the address) is the address of the current AVG. This field is also displayed under the forwarder section where it indicates the address of the current AVF.
Standby is	Standby state of the virtual gateway. The value can be local, unknown, or an IP address. The address (and the expiration date of the address) is the address of the standby gateway (the gateway that is next in line to be the AVG).
Weighting	Initial weighting value with lower and upper threshold values.
Track object	List of objects that are being tracked and their corresponding states.
Load balancing	Load-balancing method configured for the GLBP group.
Group members	List of gateways that are members of this group.
Forwarder	List of forwarders in this group.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Table 1-2 describes the fields for the **show glbp brief** command output.

Table 1-2 *show glbp brief Field Descriptions*

Field	Description
Interface	Interface type and number. GLBP group number for the interface.
Grp	GLBP group number for the interface.
Fwd	Number of forwarders in the GLBP group.
Pri	Configured priority for this gateway.
State is	State of the virtual gateway. For a virtual gateway, the state can be one of the following: • Active—The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. • Disabled—The virtual IP address has not been configured or learned yet, but another GLBP configuration exists. • Initial—The virtual IP address has been configured or learned, but the virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured. • Listen—The virtual gateway is receiving hello packets and is ready to change to the Speak state if the active or standby virtual gateway becomes unavailable. • Speak—The virtual gateway is attempting to become the active or standby virtual gateway. • Standby—The gateway is next in line to be the AVG. For a virtual forwarder, the state can be one of the following: • Active—The gateway is the active virtual forwarder (AVF) and is responsible for forwarding packets sent to the virtual forwarder MAC address. • Disabled—The virtual MAC address has not been assigned or learned. This state is transitory because a virtual forwarder that changes to a disabled state is deleted. • Initial—The virtual MAC address is known, but the virtual forwarder configuration is not complete. An interface must be up and configured to route IP, an interface IP address must be configured, and the virtual IP address must be known. • Listen—The virtual forwarder is receiving hello packets and is ready to change to the Active state if the AVF becomes unavailable.
Address	Virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If a virtual IP address is a duplicate of an address configured for another device, it will be marked as a duplicate. A duplicate address indicates that the router has failed to defend its ARP cache entry.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-2 ***show glbp brief Field Descriptions (continued)***

Field	Description
Active router	IP address of the AVG.
Standby router	IP address of the standby virtual gateway.

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp timers	Configures the time between hello messages and the time before other routers declare the active GLBP router to be down.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show glbp capability

To display which interfaces support Gateway Load Balancing Protocol (GLBP), use the **show glbp capability** command.

show glbp [*interface type number*] [*port-channel number*] [*vlan number*]

Syntax Description

interface type number	(Optional) Specifies the interface for which output is displayed.
port-channel number	(Optional) Specifies the port channel for which output is displayed.
vlan number	(Optional) VLAN for which output is displayed.

Command Modes

Any

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show glbp capability** command to display which interfaces support GLBP.
This command does not require a license.

Examples

This example shows how to display the interfaces that support GLBP:

```
switch# show glbp capability
Nexus 7010 (10 Slot) Chassis * means interface may support GLBP

Interface                               Type | Potential Max Groups
-----|-----
Eth1/1 2 Gigabit Ethernet * 1024
Eth1/2 2 Gigabit Ethernet * 1024
Eth2/1 2 Gigabit Ethernet * 1024
Eth2/2 2 Gigabit Ethernet * 1024
Eth2/3 2 Gigabit Ethernet * 1024
Eth2/4 2 Gigabit Ethernet * 1024
Eth2/5 2 Gigabit Ethernet * 1024
Eth2/6 2 Gigabit Ethernet * 1024
Eth2/7 2 Gigabit Ethernet * 1024
Eth2/8 2 Gigabit Ethernet * 1024
mgmt0 5 Management Sup Port 0
Eth Inband Port 21 Inband Port 0
Eth Inband Port 21 Inband Port 0
Eth Inband Port 21 Inband Port 0
```

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-3 describes the significant fields shown in the output.

Table 1-3 *show glbp capability Field Descriptions*

Field	Description
Interface	Interface name.
Type	Interface type.
GLBP support (represented by the I character)	* indicates the interface may support GLBP.
Potential Max Groups	Maximum number of groups supported by this interface.

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp timers	Configures the time between hello messages and the time before other routers declare the active GLBP router to be down.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show hardware forwarding dynamic-allocation status

To display information about the ternary content addressable memory (TCAM) allocation in the Forwarding Information Base (FIB), use the **show hardware forwarding dynamic-allocation status** command.

show hardware forwarding dynamic-allocation status

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **show hardware forwarding dynamic-allocation status** command to display the TCAM allocation for one or more modules.

This command does not require a license.

Examples

The following example shows how to display the TCAM allocation:

```
switch(config)# show hardware forwarding dynamic-allocation status
slot 7
=====

Num 288 bit blocks : 1 (Same as default setting)
Num 144 bit blocks : 8 (Same as default setting)
Num 72 bit blocks : 7 (Same as default setting)

slot 12
=====

Num 288 bit blocks : 1 (Same as default setting)
Num 144 bit blocks : 7 (Different from default setting)
Num 72 bit blocks : 9 (Different from default setting)
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	hardware forwarding dynamic-allocation	Configures dynamic TCAM allocation for each module.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show hardware forwarding ip verify

To display information about IP packet verification, use the **show hardware forwarding ip verify** command.

show hardware forwarding ip verify

Syntax Description This command has no keywords or arguments

Command Modes Any

Supported User Roles network-admin
VDC administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples The following example shows IP packet verification settings:

```
switch# show hardware forwarding ip verify
IPv4 and v6 IDS Checks      Status      Packets Failed
-----+-----+-----
address source broadcast    Enabled     0
address source multicast    Enabled     0
address destination zero    Enabled     0
address identical           Enabled     0
address source reserved     Enabled     0
address class-e              Disabled    0
checksum                    Enabled     0
protocol                    Enabled     0
fragment                    Enabled     0
length minimum              Enabled     0
length consistent            Enabled     0
length maximum max-frag     Enabled     0
length maximum udp          Disabled    0
length maximum max-tcp      Enabled     0
tcp flags                    Disabled    0
tcp tiny-frag               Enabled     0
version                      Enabled     0
-----+-----+-----
IPv6 IDS Checks             Status      Packets Failed
-----+-----+-----
length consistent            Enabled     0
length maximum max-frag     Enabled     0
length maximum udp          Disabled    0
length maximum max-tcp      Enabled     0
```

Send document comments to nexus7k-docfeedback@cisco.com

tcp tiny-frag	Enabled	0
version	Enabled	0

Related Commands

Command	Description
platform ip verify address	Configures IPv4 and IPv6 packet verification checks based on addresses.
platform ip verify length	Configures IPv4 packet verification checks based on length.
platform ipv6 verify	Configures IPv6 packet verification.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show hsrp

To display Hot Standby Router Protocol (HSRP) information for each HSRP group, use the **show hsrp** command.

```
show hsrp [interface type number] [group group-number] [active | init | listen | standby] [all]
[brief] [detail] [ipv4]
```

Syntax Description		
interface <i>type number</i>	(Optional) Specifies the interface type and number for which to display HSRP information.	
group <i>group-number</i>	(Optional) Specifies the HSRP group number of the interface to display information about.	
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 Modes Any

Supported User Roles network-admin
VDC administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added ipv4 keyword.
	4.2(1)	Added detail keyword.

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.

This command does not require a license.

Examples The following example shows how to display a brief summary of HSRP information:

```
switch# show hsrp brief
```

P indicates configured to preempt.

Send document comments to nexus7k-docfeedback@cisco.com

| P indicates configured to preempt.

Interface	Grp	Prio	P	State	Active addr	Standby addr	Group addr

Related Commands

Command	Description
feature hsrp	Enables the HSRP feature.

Send document comments to nexus7k-docfeedback@cisco.com

show hsrp delay

To display Hot Standby Router Protocol (HSRP) group delay information, use the **show hsrp delay** command.

show hsrp delay [*interface type number*] [**group** *group-number*] [**all**] [**brief**]

Syntax Description

interface <i>type number</i>	(Optional) Specifies the interface type and number for which to display HSRP information.
group <i>group-number</i>	(Optional) Specifies the HSRP group number of the interface to display information about.

Command Modes

Any

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show hsrp delay** command to display delay information about HSRP groups. This command does not require a license.

Examples

The following example shows how to display GLBP delay information:

```
switch# show hsrp delay
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 keywords or arguments.

Command Modes	Any

Supported User Roles	network-admin VDC administrator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	Use the show hsrp summary command to display summary information about HSRP groups. This command does not require a license.

Examples	The following example shows how to display a summary of HSRP information:

```
switch# show hsrp summary

PHSRP Summary:
-----
Extended-hold (NSF) disabled

Total Groups: 1
  Version:: V1-IPV4: 1    V2-IPV4: 0
  State::   Active: 0    Standby: 0    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: 142
-----
```

Related Commands

 show hsrp summary

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
feature hsrp	Enables the HSRP feature.

Send document comments to nexus7k-docfeedback@cisco.com

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*]

Syntax Description	<i>ip-addr</i>	(Optional) An IPv4 source address. The format is x.x.x.x.
	<i>interface</i>	(Optional) An 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.
	<i>vrf vrf-name</i>	(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

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(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. This command does not require a license.

Examples	This example displays a summary of the adjacency information: <pre>switch# show ip adjacency summary</pre> IP AM Table - Adjacency Summary <pre>Static : 1 Dynamic : 22 Others : 0 Total : 23</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show forwarding adjacency	Displays forwarding adjacency information.

Send document comments to nexus7k-docfeedback@cisco.com

show ip arp

To display the Address Resolution Protocol (ARP) information, use the **show ip arp** command.

show ip arp [*ip-addr* | *interface*] [**client**] [**static**] [**statistics**] [**summary**] [**vrf** *vrf-name*]

Syntax Description	<i>ip-addr</i>	(Optional) An IPv4 source address. The format is x.x.x.x.
	<i>interface</i>	(Optional) An interface. Use ? to determine the supported interface types.
	client	(Optional) Displays the ARP client table
	static	(Optional) Displays static ARP entries.
	statistics	(Optional) Displays ARP statistics.
	summary	(Optional) Displays a summary of the ARP table.
	vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays a summary of the ARP table:

```
switch# show ip arp summary

IP ARP Table - Adjacency Summary

Resolved   : 33
Incomplete : 0
Unknown    : 0
Total      : 33
```

 show ip arp

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
ip arp timeout	Configures ARP.

Send document comments to nexus7k-docfeedback@cisco.com

show ip as-path-access-list

To display the AS Path access lists for the Border Gateway Protocol (BGP), use the **show ip as-path-access-list** command.

show ip as-path-access-list [*name*]

Syntax	Description	
	<i>name</i>	(Optional) AS path access list name. The name can be any case-sensitive alphanumeric string up to 63 characters.
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the AS path access lists: switch# show ip as-path-access-list ip as-path access-list Test1 permit "10.0.0.1"	
Related Commands	Command	Description
	ip as-path access-list	Configures an AS path access list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>ip-addr</i>	(Optional) A network from the BGP route table. The format is x.x.x.x.
<i>ip-prefix</i>	(Optional) A prefix from the 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 <i>expression</i>	(Optional) Display information that matches the regular expression.
route-map <i>map-name</i>	(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 <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the BGP route table:

```
switch(config-router)# show ip bgp
BGP routing table information for VRF default, address family IPv4 Unicast
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
clear ip bgp	Clears entries in the BGP route table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip bgp community-list

To display Border Gateway Protocol (BGP) routes that match a 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) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv6 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display 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 63 characters.

Defaults None

Command Modes Any command mode

Supported User Roles

- network-admin
- network-operator
- vdc-admin
- vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example displays routes that match a community list:

```
switch(config)# show ip bgp community-list test1
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
ip community-list	Creates a community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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** [**regex** *expression*] | **flap-statistics** | **history-paths** [**regex** *expression*] | **parameters**} [**vrf** *vrf-name*]

Syntax Description	
ipv4	(Optional) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv4 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display BGP information for all address families.
dampened-paths	Display all dampened paths.
regex <i>expression</i>	(Optional) Display information that matches the regular expression.
flap-statistics	Display flap statistics for routes.
history-paths	Display all history paths.
parameters	Display all dampening parameters.
vrf <i>vrf-name</i>	(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

Supported User Roles

- network-admin
- network-operator
- vdc-admin
- vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example displays dampening information:

```
switch(config)# show ip bgp dampening dampened-paths
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show ipv6 bgp dampening	Displays BGP dampening information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 specific extended communities.
	non-transitive	Displays the routes that match the non-transitive extended communities.
	transitive	Displays the routes that match the transitive extended communities.
	<i>as4-number</i>	AS number. The <i>as4-number</i> 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.

Defaults	None

Command Modes	Any command mode

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays 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.

Send document comments to nexus7k-docfeedback@cisco.com

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	<table> <tr> <td><i>commlist-name</i></td><td>Name of an extended community-list. The <i>commlist-name</i> can be any case-sensitive alphanumeric string up to 63 characters.</td></tr> <tr> <td>exact-match</td><td>(Optional) Displays an exact match of the extended communities.</td></tr> <tr> <td>vrf <i>vrf-name</i></td><td>(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.</td></tr> </table>	<i>commlist-name</i>	Name of an extended community-list. The <i>commlist-name</i> can be any case-sensitive alphanumeric string up to 63 characters.	exact-match	(Optional) Displays an exact match of the extended communities.	vrf <i>vrf-name</i>	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>commlist-name</i>	Name of an extended community-list. The <i>commlist-name</i> can be any case-sensitive alphanumeric string up to 63 characters.						
exact-match	(Optional) Displays an exact match of the extended communities.						
vrf <i>vrf-name</i>	(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						
Supported User Roles	network-admin network-operator vdc-admin vdc-operator						
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>4.2(1)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	4.2(1)	This command was introduced.		
Release	Modification						
4.2(1)	This command was introduced.						
Usage Guidelines	This command does not require a license.						
Examples	This example displays routes that match a community list: <pre>switch(config)# show ip bgp extcommunity-list test1</pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>ip extcommunity-list</td><td>Creates an extended community list.</td></tr> </table>	Command	Description	ip extcommunity-list	Creates an extended community list.		
Command	Description						
ip extcommunity-list	Creates an extended community list.						

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>list-name</i>	Name of a filter-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 <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a filter list: switch(config)# show ip bgp filter-list test1

Related Commands	Command	Description
	show ipv6 bgp filter-list	Displays BGP routes that match a filter list.

Send document comments to nexus7k-docfeedback@cisco.com

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 [*prefix*] [**vrf** *vrf-name*]

Syntax Description	<i>prefix</i>	(Optional) IPv6 prefix. The format is x.x.x.x/length.
	vrf <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the flap statistics:	
	switch(config)# show ip bgp flap-statistics	
Related Commands	Command	Description
	show ipv6 bgp	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip bgp history-paths

To display Border Gateway Protocol (BGP) history paths, use the **show ip bgp history-paths** command.

show ip bgp [**ipv4** {**unicast** | **multicast**} | **all**] **history-paths** [**regex** *expression*] [**vrf** *vrf-name*]

Syntax	Description
ipv4	(Optional) Display BGP information for IPv4 address family.
ipv6	(Optional) Display BGP information for IPv6 address family.
unicast	Displays BGP information for unicast address family.
multicast	Displays BGP information for multicast address family.
all	(Optional) Display BGP information for all address families.
regex <i>expression</i>	(Optional) Display information that matches the regular expression.
vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays BGP history path information: <pre>switch(config)# show ip bgp history-paths</pre>

Related Commands	Command	Description
	show ipv6 bgp history-paths	Displays BGP history paths information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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]] | prefix] [vrf { all | vrf-name }]
```

Syntax Description	
<i>addr</i>	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.
<i>prefix</i>	(Optional) IPv6 prefix. The format is x.x.x.x/length.
vrf <i>vrf-name</i>	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
all	(Optional) Specifies all VRFS.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added paths keyword.

Usage Guidelines	This command does not require a license.

Examples	This example displays the BGP neighbors:

 show ip bgp neighbors

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# show ip bgp neighbors
```

Related Commands

Command	Description
show ipv6 bgp neighbors	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>addr</i>	IPv4 address. The format is x.x.x.x
	vrf <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the BGP next-hop information: switch(config)# show ip bgp nexthop 192.0.2.1	
Related Commands	Command	Description
	show ipv6 bgp nexthop	Displays BGP information.

Send document comments to nexus7k-docfeedback@cisco.com

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 63 characters.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the BGP next-hop database:

```
switch(config)# show ip bgp nexthop-database
```

Related Commands

Command	Description
show ipv6 bgp nexthop-database	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>name</i>	Name of a BGP template. The name can be any case-sensitive alphanumeric string up to 63 characters.
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the BGP peer policy: <pre>switch(config)# show ip bgp peer-policy test1</pre> Commands configured in this template: <pre>Send Community Suppress Inactive Default Originate - route-map:</pre> Inherited commands: Inherited by the following peers: <pre>VRF default: 192.0.2.3</pre>	
Related Commands	Command	Description
	inherit peer-policy	Inherits a peer policy template for a neighbor.
	template peer-policy	Configures a peer policy template.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>name</i>	Name of a BGP template. The name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any command mode

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays the BGP peer session: <pre>switch(config)# show ip bgp peer-session test1</pre> Commands configured in this template: <pre> Update Source - interface: Vlan33 EBGp Multihop - hop limit: 33</pre> Inherited commands: Inherited by the following peers: <pre> VRF default: 192.0.2.3</pre>

Related Commands	Command	Description
	inherit peer-session	Inherits a peer session template for a neighbor.
	template peer-session	Configures a peer session template.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>name</i>	Name of a BGP template. The name can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any command mode

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays the BGP peer template: <pre>switch(config)# show ip bgp peer-template peer1 BGP peer-template is peer1 Connected check is disabled Hold time = 0, keepalive interval is 0 seconds Message statistics: Sent Rcvd Opens: 0 0 Notifications: 0 0 Updates: 0 0 Keepalives: 0 0 Route Refresh: 0 0 Capability: 0 0 Total: 0 0 Total bytes: 0 0 Bytes in queue: 0 0 Members of peer-template peer1: default:192.0.2.3</pre>

 show ip bgp peer-template

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
inherit peer-template	Inherits a peer template for a neighbor.
template peer	Configures a peer template.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>list-name</i>	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 <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays routes that match a prefix list: switch(config) # show ip bgp prefix-list test1	
Related Commands	Command	Description
	show ipv6 bgp prefix-list	Displays BGP routes that match a prefix list.

Send document comments to nexus7k-docfeedback@cisco.com

show ip client

To display information about the internal IP clients, use the **show ip client** command.

show ip client [*name*]

Syntax Description	<i>name</i> (Optional) Name of client.	
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the IP client information for ARP: <pre>switch(config)# show ip client arp</pre> Client: arp, uuid: 268, pid: 3687, extended pid: 3687 Protocol: (none), client-index: 2, routing VRF id: 255 Data MTS-SAP: 0 Data messages, send successful: 33, failed: 0	
Related Commands	Command	Description
	show ip process	Displays information about the IP process.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>name</i> (Optional) Name of community list. The name can be any case-sensitive alphanumeric string up to 63 characters.				
Defaults	None				
Command Modes	Any command mode				
Supported User Roles	network-admin network-operator vdc-admin vdc-operator				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
Usage Guidelines	This command does not require a license.				
Examples	This example displays the community lists: <pre>switch(config)# show ip community-list Standard Community List test2 permit internet local-AS</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip community-list</td><td>Configures a BGP community list.</td></tr></table>	Command	Description	ip community-list	Configures a BGP community list.
Command	Description				
ip community-list	Configures a BGP community list.				

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The <i>instance-tag</i> can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	This example displays all the EIGRP instances:

```
switch# show ip eigrp
IP-EIGRP AS 0 ID 0.0.0.0 VRF default
  Process-tag: Test1
  Status: shutdown
  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: 0 (0 loopbacks)
  Number of EIGRP peers: 0
IP-EIGRP AS 0 ID 0.0.0.0 VRF default
  Process-tag: Test2
  Status: shutdown
  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: 0 (0 loopbacks)
```


Send document comments to nexus7k-docfeedback@cisco.com

Number of EIGRP peers: 0

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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* | *}]

Syntax Description

<i>instance-tag</i>	(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 63 characters.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the EIGRP accounting information:

```
switch# show ip eigrp accounting
```

```
IP-EIGRP accounting for AS(100)/ID(192.0.2.1) vrf RED
Total Prefix Count: 4
States: A-Adjacency, P-Pending, D-Down
```

State	Address/Source	Interface	Prefix Count	Restart Count	Restart/Reset (s)
P	Redistributed	----	0	3	211
A	192.0.2.2	e2/1	2	0	84
P	192.0.2.4	e3/3	0	2	114
D	192.0.2.3	e4/1	0	3	0

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-4 describes the significant fields shown in the display.

Table 1-4 *show ip eigrp accounting* Field Descriptions

Field	Description
IP-EIGRP accounting for AS...	EIGRP instance, AS number, router ID, and table ID.
Total Prefix Count:	Aggregate sum of the prefixes in an EIGRP instance topology table. The count includes prefixes learned from all neighbors or from redistribution.
States: A-Adjacency, P-Pending, D-Down	A-Adjacency: Indicates a stable adjacency with the neighbor or a normal redistribution state. P-Pending: Neighbor adjacency or redistribution is suspended or in a penalized state because the maximum prefix limit was exceeded. D-Down: Neighbor adjacency or redistribution is suspended permanently until a manual reset is performed with the clear route command.
Address/Source	Peer IP address of the redistribution source.
Prefix Count	Total number of learned prefixes by source. Note Routes can be learned for the same prefix from multiple sources, and the sum of all prefix counts in this column may be greater than the figure displayed in the “Prefix Count” field.
Restart Count	Number of times that a route source exceeded the maximum prefix limit.
Restart Reset(s)	Time, in seconds, that a route source is in a P (penalized) state. If the route source is in an A (stable or normal) state, the displayed time, in seconds, is the time period until penalization history is reset.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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** [*type instance*] [**brief**] [**vrf** {*vrf-name* | *}]

Syntax Description

<i>instance-tag</i>	(Optional) instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance. Specifying <i>instance</i> removes all entries learned through this interface from the neighbor table. The <i>instance</i> argument has the following syntax: - Physical interface instance. Naming notation is <i>slot/port</i> and a slash mark between values is required as part of the notation. - Virtual interface instance. The number range varies depending on the interface type. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Displays brief summary of EIGRP interface information.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults

This command shows all interfaces for the default VRF if no VRF or no interface is specified.

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	Added brief keyword.

Send document comments to nexus7k-docfeedback@cisco.com

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 Enterprise Services license.

Examples

The following example shows how to display information about EIGRP interfaces:

```
switch# show ip eigrp interfaces brief
```

```
IP EIGRP interfaces for process 1 vrf default
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
e2/2	0	0/0	0	11/434	0	0
e2/20	1	0/0	337	0/10	0	0
e4/2	1	0/0	10	1/63	103	0
e3/2	1	0/0	330	0/16	0	0

```
switch#
```

[Table 1-5](#) describes the significant fields shown in the display.

Table 1-5 *show ip eigrp interfaces Field Descriptions*

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.
Xmit Queue Un/Reliable	Number of packets remaining in the unreliable and reliable transmit queues.
Mean SRTT	Mean smoothed round-trip time (SRTT) internal (in milliseconds).
Pacing Time Un/Reliable	Pacing time used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the router sends multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.

Related Commands

Command	Description
show ip eigrp neighbors	Displays the neighbors discovered by EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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] [interface-type interface-instance] [static] [vrf
{ vrf-name | * }]
```

Syntax Description

<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
detail	(Optional) Displays detailed EIGRP neighbor information.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance. Specifying <i>instance</i> removes all entries learned through this interface from the neighbor table. The <i>instance</i> argument has the following syntax: - Physical interface instance. Naming notation is <i>slot/port</i> and a slash mark between values is required as part of the notation. - Virtual interface instance. The number range varies depending on the interface type. For more information about the syntax for the router, use the question mark (?) online help function.
static	(Optional) Displays static EIGRP interface information.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults

This command displays all neighbors for the default VRF on all interfaces if no VRF or interface is specified.

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

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 Enterprise Services license.

Examples

The following example shows how to display information about EIGRP neighbors:

```
switch# show ip eigrp neighbors
```

```
IP-EIGRP Neighbors for process 77 vrf default
```

Address	Interface	Holdtime (secs)	Uptime (h:m:s)	Q Count	Seq Num	SRTT (ms)	RTO (ms)
192.0.2.28	e1/3	13	0:00:41	0	11	4	20
192.0.2.2	e4/4	14	0:02:01	0	10	12	24

```
switch#
```

[Table 1-6](#) describes the significant fields shown in the display.

Table 1-6 *show ip eigrp neighbors Field Descriptions*

Field	Description
process	Autonomous system number specified in the router configuration command.
vrf	VRF name.
Address	IP address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Holdtime	Length of time (in seconds) that the Cisco NX-OS software waits to hear from the peer before declaring that the peer is down.
Uptime	Elapsed time (in hours, minutes, and seconds) since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the software waits to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
SRTT	Smoothed round-trip time. This field indicates the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This field indicates the amount of time that the software waits before resending a packet from the retransmission queue to a neighbor.

The following example shows how to display detailed information about EIGRP neighbors:

```
switch# show ip eigrp neighbors detail
```

■ show ip eigrp neighbors

Send document comments to nexus7k-docfeedback@cisco.com

```
IP-EIGRP neighbors for AS 1 vrf default
```

```

H   Address                Interface      Hold Uptime    SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt  Num
0   192.0.2.10              e1/5          14 01:00:52    3     200   0   10

```

```
Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 3
```

```
switch#
```

[Table 1-7](#) describes the significant fields shown in the display.

Table 1-7 *show ip eigrp neighbors detail Field Descriptions*

Field	Description
Version	Version of EIGRP software running on the node and neighbor.
Retrans:	Number of retransmissions sent to this neighbor.
Retries:	Number of retransmissions sent to this neighbor since the last acknowledgement (ACK).
Prefixes	Number of prefixes learned from this neighbor.

Related Commands

Command	Description
clear ip eigrp neighbors	Clears neighbors for EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip eigrp policy statistics

To display the policy statistics for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ip eigrp policy statistics** command in any mode.

```
show ip eigrp [instance-tag] policy statistics redistribute {bgp id | direct | eigrp id | isis id | ospf
id | rip id | static} [vrf {vrf-name | *}]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 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.
isis	Displays policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
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.
<i>id</i>	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 NX-OS stores it internally as a string. For the isis keyword, an IS-IS 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 NX-OS 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(13)	This command was removed and replaced by the show ip eigrp route-map statistics command.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to display policy statistics for EIGRP:

```
switch(config)# show ip eigrp policy statistics redistribute direct
C: No. of comparisons, M: No. of matches

route-map rmap1 permit 1

Total accept count for policy: 10
Total reject count for policy: 0
```

Related Commands

Related Commands

Command	Description
clear ip eigrp policy statistics	Clears policy statistics for EIGRP.
show ip eigrp traffic	Displays EIGRP traffic statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 | isis id
| ospf id | rip id | static} vrf {vrf-name | *}]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 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.
isis	Displays policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
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.
<i>id</i>	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 NX-OS stores it internally as a string. For the isis keyword, an IS-IS 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 NX-OS 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command replaces the **show ip eigrp policy statistics** command. This command does not require a license.

Examples

The following example shows how to display route-map statistics for EIGRP:

```
switch(config)# show ip eigrp route-map statistics redistribute direct
C: No. of comparisons, M: No. of matches

route-map rmap1 permit 1

Total accept count for policy: 10
Total reject count for policy: 0
```

Related Commands

Related Commands

Command	Description
clear ip eigrp route-map statistics	Clears route-map statistics for EIGRP.
show ip eigrp traffic	Displays EIGRP traffic statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 | *}]
```

Syntax	Description
<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
<i>ip-address/length</i>	(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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults	This command displays information for the default VRF if no VRF is specified.

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

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 NX-OS displays only routes that are feasible successors.

This command requires the Enterprise 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 1): Topology entry for 192.0.2.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
  Routing Descriptor Blocks:
    192.0.2.22 (Ethernet 2/1), from 192.0.2.1, Send flag is 0x0
      Composite metric is (409600/128256), Route is External
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 10.89.245.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
switch#
```

This example show the **all-links** option:

```
switch(config)# show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(100)/ID(4.4.4.4) VRF default

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 3.3.3.0/24, 1 successors, FD is 130816, serno 58
   via 192.168.6.2 (130816/128256), Ethernet2/2
   via 192.168.5.2 (153856/128256), Ethernet2/1
P 2.2.2.0/24, 1 successors, FD is 130816, serno 57
   via 192.168.6.2 (130816/128256), Ethernet2/2
   via 192.168.5.2 (153856/128256), Ethernet2/1
P 1.1.1.0/24, 1 successors, FD is 130816, serno 56
   via 192.168.6.2 (130816/128256), Ethernet2/2
   via 192.168.5.2 (153856/128256), Ethernet2/1
P 192.168.6.0/24, 1 successors, FD is 2816, serno 25
   via Connected, Ethernet2/2
   via 192.168.5.2 (26112/2816), Ethernet2/1
P 6.6.6.0/24, 1 successors, FD is 128256, serno 24
   via Connected, loopback6
P 5.5.5.0/24, 1 successors, FD is 128256, serno 23
   via Connected, loopback5
P 4.4.4.0(1)/24, 1 successors, FD is 128256, serno 16
   via Connected, loopback4
P 192.168.5.0/24, 1 successors, FD is 25856, serno 1
   via Connected, Ethernet2/1
   via 192.168.6.2 (3072/2816), Ethernet2/2
```

Send document comments to nexus7k-docfeedback@cisco.com

This example shows more details:

```
switch(config)# show ip eigrp topology detail-links
IP-EIGRP Topology Table for AS(100)/ID(4.4.4.4) VRF default

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 3.3.3.0/24, 1 successors, FD is 130816, serno 58
    via 192.168.6.2 (130816/128256), Ethernet2/2
    via 192.168.5.2 (153856/128256), Ethernet2/1
P 2.2.2.0/24, 1 successors, FD is 130816, serno 57
    via 192.168.6.2 (130816/128256), Ethernet2/2
    via 192.168.5.2 (153856/128256), Ethernet2/1
P 1.1.1.0/24, 1 successors, FD is 130816, serno 56
    via 192.168.6.2 (130816/128256), Ethernet2/2
    via 192.168.5.2 (153856/128256), Ethernet2/1
P 192.168.6.0/24, 1 successors, FD is 2816, serno 25
    via Connected, Ethernet2/2
    via 192.168.5.2 (26112/2816), Ethernet2/1
P 6.6.6.0/24, 1 successors, FD is 128256, serno 24
    via Connected, loopback6
P 5.5.5.0/24, 1 successors, FD is 128256, serno 23
    via Connected, loopback5
P 4.4.4.0(1)/24, 1 successors, FD is 128256, serno 16
    via Connected, loopback4
P 192.168.5.0/24, 1 successors, FD is 25856, serno 1
    via Connected, Ethernet2/1
    via 192.168.6.2 (3072/2816), Ethernet2/2
```

This example shows a summary of the topology table:

```
switch(config)# show ip eigrp topology summary
IP-EIGRP Topology Table for AS(100)/ID(4.4.4.4) VRF default

Head serial 1, next serial 59
8 routes, 0 pending replies, 0 dummies
IP-EIGRP(0) enabled on 5 interfaces, 2 neighbors present on 2 interfaces
Quiescent interfaces:  Eth2/2 Eth2/1
```

This example shows the active entries in the topology table:

```
switch(config-if)# show ip eigrp topology active
IP-EIGRP Topology Table for AS(101)/ID(80.86.2.3) VRF default

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

A 8.3.2.0/24, 1 successors, FD is Inaccessible
    1 replies, active 00:00:04, query-origin: Local origin
    via Connected (Infinity/Infinity), loopback8
    Remaining replies:
    via 5.5.5.6, r, Ethernet2/6
```

This example shows zero-successors in the topology table:

```
switch(config-router)# show ip eigrp topology zero-successors
IP-EIGRP Topology Table for AS(101)/ID(10.1.48.4) VRF default

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.1.49.0/24, 0 successors, FD is Inaccessible
    via 5.5.5.5 (28416/28160), Ethernet2/6
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

This example shows pending entries:

```
switch(config)# show ip eigrp topology pending
IP-EIGRP Topology Table for AS(100)/ID(1.1.1.1) VRF default

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 6.6.6.0/24, 1 successors, FD is 130816, U
    via 192.168.5.1 (130816/128256), Ethernet2/1
P 5.5.5.0/24, 1 successors, FD is 130816, U
    via 192.168.5.1 (130816/128256), Ethernet2/1
P 4.4.4.0(1)/24, 1 successors, FD is 130816, U
    via 192.168.5.1 (130816/128256), Ethernet2/1
P 8.8.8.0/24, 1 successors, FD is 130816, U
    via 192.168.5.1 (130816/128256), Ethernet2/1
```

Table 1-8 describes the significant fields shown in the display.

Table 1-8 *show ip eigrp topology Field Descriptions*

Field	Description
Query origin	Query origin state.
Successors	Number of feasible successors for this prefix.
FD	Feasible distance for this prefix.
192.0.2.22(Ethernet 2/1)	Next hop and interface from which this path was learned.
from 192.0.2.1	Information source for this path.
Send flag	Status of whether the sending of this prefix is pending to this neighbor.
Composite metric is...	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.
Route is	Type of route (internal or external).
Vector Metric	Metric (bandwidth, delay, reliability, load, MTU, and hop count) advertised by the neighbor.
External Data	External information (originating router ID, AS number, external protocol, metric, and tag) advertised by the neighbor.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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* | *}]

Syntax Description	<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
	vrf *	(Optional) Specifies all VRF instances.

Defaults	This command displays information for the default VRF if no VRF is specified.

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following example shows how to display the EIGRP traffic statistics:

```
switch# show ip eigrp traffic
```

```
IP-EIGRP Traffic Statistics for AS 1 vrf default
```

```
Hellos sent/received: 736/797
Updates sent/received: 6/6
Queries sent/received: 0/1
Replies sent/received: 1/0
Acks sent/received: 6/6
```

Send document comments to nexus7k-docfeedback@cisco.com

```
Input queue high water mark 0, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
```

Table 1-9 describes the significant fields shown in the display.

Table 1-9 *show ip eigrp traffic Field Descriptions*

Field	Description
AS	Autonomous system number specified in the router eigrp command.
vrf	VRF specified in the show command.
Hellos sent/received:	Number of hello packets sent and received.
Updates sent/received:	Number of update packets sent and received.
Queries sent/received:	Number of query packets sent and received.
Replies sent/received:	Number of reply packets sent and received.
Acks sent/received:	Number of acknowledgment packets sent and received.
Input queue high water mark	Maximum number of packets in the input queue and number of drops.
SIA-Queries sent/received	Number of Stuck-in-Active query packets sent and received.
SIA-Replies sent/received:	Number of Stuck-in-Active reply packets sent and received.

Send document comments to nexus7k-docfeedback@cisco.com

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	(Optional) Displays the forwarding information for routes on a module.
	module <i>slot</i>	Displays information for the module. The slot range depends on the hardware platform.

Command Modes	Any

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(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.

This command does not require a license.

Examples	This example displays forwarding information for module 2:

```
switch# show ip fib route module 2
```

```
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
```

Related Commands	Command	Description
	show forwarding	Displays information about the FIB.

Send document comments to nexus7k-docfeedback@cisco.com

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 Modes	Any

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays forwarding information for unicast clients:

```
switch# show ip fib distribution clients
```

```

id  pid    shmem-start  shmem-end  shmem-name
--  -
1   3646    0x64f70120  0x64fc0000  u6rib-ufdm
2   3647    0x64b50120  0x64d50000  urib-ufdm

```

Related Commands	Command	Description
	show forwarding distribution	Displays distribution information about the FIB.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>type</i>	(Optional) Interface type. Use ? to see the options.
	<i>number</i>	(Optional) Interface number. Use ? to see the range.
	brief	(Optional) Displays a summary of IP information.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Modes	Any

SupportedUserRoles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays IP information for Ethernet 2/1:

```
switch# show ip interface ethernet 2/1
Ethernet2/1, Interface status: protocol-down/link-down/admin-down, iof: 80,
  IP VRF context: "default"
  IP address: 192.0.2.1, IP subnet: 192.0.0.0/8
  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 unreachable (except port): disabled
  IP icmp port-unreachable: enabled
  IP RP inbound packet-filtering policy: none
  IP RP outbound packet-filtering policy: none
  IP inbound packet-filtering policy: none
  IP outbound packet-filtering policy: none
  IP unicast reverse path forwarding: none
```

Send document comments to nexus7k-docfeedback@cisco.com

```
IP unicast reverse path forwarding fail policy: 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
  Labeled packets      : 0/0/0/0/0
  Labeled bytes        : 0/0/0/0/0
```

Related Commands

Command	Description
show ipv6 interface	Displays IPv6 information about an interface.

Send document comments to nexus7k-docfeedback@cisco.com

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 Modes	Any

SupportedUserRoles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays IP load sharing information:

```
switch# show ip load-sharing
IPv4/IPv6 ECMP load sharing:
Universal-id (Random Seed): 2823428857
Load-share mode : address source-destination port source-destination Broadcast bytes      :
0/0/0/0/0
    Labeled packets      : 0/0/0/0/0
    Labeled bytes        : 0/0/0/0/0
```

Related Commands	Command	Description
	show ip load-sharing	Displays IP load sharing.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp

To display entries in the Multiprotocol Border Gateway Protocol (MP-BGP) table, use the **show ip mbgp** command.

```
show ip mbgp [p-addr | ip-prefix [longer-prefixes]] [received-paths] [regex expression]
[route-map map-name] [summary] [vrf vrf-name]
```

Syntax Description	
<i>ip-addr</i>	(Optional) A network from the MBGP route table. The format is x.x.x.x.
<i>ip-prefix</i>	(Optional) A prefix from the the MBGP 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.
regex <i>expression</i>	(Optional) Display information that matches the regular expression.
route-map <i>map-name</i>	(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 <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays the MBGP route table: <pre>switch(config-router)# show ip mbgp BGP routing table information for VRF default, address family IPv4 Multicast</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	clear ip mbgp	Clears entries in the MBGP route table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp community

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match a community, use the **show ip mbgp community** command.

show ip mbgp community [*as-number*] [**internet**] [**no-advertise**] [**no-export**]
[**no-export-subconfed**] [**exact-match**]} [**vrf** *vrf-name*]

Syntax Description

<i>as-number</i>	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>.
internet	(Optional) Displays the internet community.
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.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays routes that match a community:

```
switch(config)# show ip mbgp community
```

Related Commands

Command	Description
ip community-list	Creates a community list.

Send document comments to nexus7k-docfeedback@cisco.com

show ip mbgp community-list

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match a community list, use the **show ip mbgp community-list** command.

show ip mbgp community-list *commlist-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description	<i>commlist-name</i>	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 <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a community list: <pre>switch(config)# show ip mbgp community-list test1</pre>

Related Commands	Command	Description
	ip community-list	Creates a community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp dampening

To display Multiprotocol Border Gateway Protocol (MP-BGP) dampening information, use the **show ip mbgp dampening** command.

show ip mbgp dampening { **dampened-paths** [**regex** *expression*] | **flap-statistics** | **history-paths** [**regex** *expression*] | **parameters** } [**vrf** *vrf-name*]

Syntax Description	
ipv4	(Optional) Display MBGP information for IPv4 address family.
ipv6	(Optional) Display MBGP information for IPv6 address family.
unicast	Displays MBGP information for unicast address family.
multicast	Displays MBGP information for multicast address family.
all	(Optional) Display MBGP information for all address families.
dampened-paths	Display all dampened paths.
regex <i>expression</i>	(Optional) Display information that matches the regular expression.
flap-statistics	Display flap statistics for routes.
history-paths	Display all history paths.
parameters	Display all dampening parameters.
vrf <i>vrf-name</i>	(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

Supported User Roles

- network-admin
- network-operator
- vdc-admin
- vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example displays dampening information:

```
switch(config)# show ip mbgp dampening dampened-paths
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show ipv6 bgp dampening	Displays BGP dampening information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp extcommunity

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match an extended community, use the **show ip mbgp extcommunity** command.

```
show ip mbgp extcommunity generic { non-transitive | transitive } [as4-number] [exact-match]
[vrf vrf-name]
```

Syntax Description	generic	Displays the routes that match the generic specific extended communities.
	non-transitive	Displays the routes that match the non-transitive extended communities.
	transitive	Displays the routes that match the transitive extended communities.
	<i>as4-number</i>	AS number. The <i>as4-number</i> 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.
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.2(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays routes that match an extended community:	
	switch(config)# show ip mbgp extcommunity generic transitive 1.3:30	
Related Commands	Command	Description
	ip extcommunity-list	Creates an extended community list.

Send document comments to nexus7k-docfeedback@cisco.com

show ip mbgp extcommunity-list

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match an extended community list, use the **show ip mbgp extcommunity-list** command.

show ip mbgp extcommunity-list *commlist-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description	<i>commlist-name</i>	Name of an extended community-list. The <i>commlist-name</i> can be any case-sensitive alphanumeric string up to 63 characters.
	exact-match	(Optional) Displays an exact match of the extended communities.
	vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a community list: switch(config)# show ip mbgp extcommunity-list test1

Related Commands	Command	Description
	ip extcommunity-list	Creates an extended community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp filter-list

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match a filter list, use the **show ip mbgp filter-list** command.

show ip mbgp filter-list *list-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description	<i>list-name</i>	Name of a filter-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 <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a filter list: switch(config)# show ip mbgp filter-list test1

Related Commands	Command	Description
	show ipv6 bgp filter-list	Displays BGP routes that match a filter list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp flap-statistics

To display Multiprotocol Border Gateway Protocol (MP-BGP) flap statistics, use the **show ip mbgp flap-statistics** command.

show ip mbgp flap-statistics [*prefix*] [**vrf** *vrf-name*]

Syntax Description

<i>prefix</i>	(Optional) IPv6 prefix. The format is x.x.x.x/length.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the flap statistics:

```
switch(config)# show ip mbgp flap-statistics
```

Related Commands

Command	Description
show ipv6 bgp	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp history-paths

To display Multiprotocol Border Gateway Protocol (MP-BGP) history paths, use the **show ip mbgp history-paths** command.

show ip mbgp history-paths [**regex** *expression*] [**vrf** *vrf-name*]

Syntax Description	regex <i>expression</i>	(Optional) Display information that matches the regular expression.
	vrf <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays BGP history path information:	
	switch(config)# show ip mbgp history-paths	
Related Commands	Command	Description
	show ipv6 bgp history-paths	Displays BGP history paths information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp neighbors

To display Multiprotocol Border Gateway Protocol (MP-BGP) neighbors, use the **show ip mbgp neighbors** command.

```
show ip bgp neighbors [ addr [advertised-routes | flap-statistics | paths | received-routes | routes  
[advertised | dampened | received]] | prefix] [vrf { all | vrf-name }]
```

Syntax Description	
<i>addr</i>	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.
<i>prefix</i>	(Optional) IPv6 prefix. The format is x.x.x.x/length.
vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
all	(Optional) Specifies all VRFS.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added paths keyword.

Usage Guidelines	This command does not require a license.

 show ip mbgp neighbors

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example displays the MBGP neighbors:

```
switch(config)# show ip mbgp neighbors
```

Related Commands

Command	Description
show ipv6 bgp neighbors	Displays BGP information.

Send document comments to nexus7k-docfeedback@cisco.com

show ip mbgp nexthop

To display Multiprotocol Border Gateway Protocol (MP-BGP) next hop information, use the **show ip mbgp nexthop** command.

show ip mbgp nexthop *addr* [**vrf** *vrf-name*]

Syntax Description	<i>addr</i>	IPv4 address. The format is x.x.x.x
	vrf <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the BGP next-hop information:	
	switch(config)# show ip mbgp nexthop 192.0.2.1	
Related Commands	Command	Description
	show ipv6 bgp nexthop	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip mbgp nexthop-database

To display Multiprotocol Border Gateway Protocol (MP-BGP) next-hop database, use the **show ip mbgp nexthop-database** command.

show ip mbgp nexthop-database [**vrf** *vrf-name*]

Syntax Description

vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the BGP next-hop database:

```
switch(config)# show ip mbgp nexthop-database
```

Related Commands

Command	Description
show ipv6 bgp nexthop-database	Displays BGP information.

Send document comments to nexus7k-docfeedback@cisco.com

show ip mbgp prefix-list

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match a prefix list, use the **show ip mbgp prefix-list** command.

show ip mbgp prefix-list *list-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description	<i>list-name</i>	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 <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays routes that match a prefix list: switch(config)# show ip mbgp prefix-list test1	
Related Commands	Command	Description
	show ipv6 bgp prefix-list	Displays BGP routes that match a prefix list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>instance-tag</i>	(Optional) Name of the OSPF instance. Use this tag to display OSPF information about a specific OSPF instance. The <i>instance-tag</i> argument can be any alphanumeric string.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following example shows how to display information about one specific OSPF instance:

```
switch# show ip ospf 201
Routing Process 201 with ID 192.0.2.15 vrf default
Stateful High Availability enabled
Graceful-restart is configured
  Notify period: 15, grace period: 60, state: Inactive
  Last graceful restart exit status: (null)
Supports only single TOS(TOS0) routes
Supports opaque LSA
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
Minimum hold time for Router LSA throttle 5000.000 ms
Minimum hold time for Network LSA throttle 5000.000 ms
```


Send document comments to nexus7k-docfeedback@cisco.com

```

Minimum LSA arrival 1000.000 msec
Maximum paths to destination 8
Number of external LSAs 0, checksum sum 0
Number of opaque AS LSA 0, checksum sum 0
Number of areas is 2, 2 normal, 0 stub, 0 nssa
Number of active areas is 0, 0 normal, 0 stub, 0 nssa
  Area BACKBONE(0) (Inactive)
    Area has existed for 1w0d
    Interfaces in this area: 1 Active interfaces: 0
    No authentication available
    SPF calculation has run 3 times
      Last SPF ran for 0.000132s
    Area ranges are
    Number of LSAs: 0, checksum sum 0
  Area (10) (Inactive)
    Area has existed for 1w0d
    Interfaces in this area: 1 Active interfaces: 0
    No authentication available
    SPF calculation has run 3 times
      Last SPF ran for 0.000035s
    Area ranges are
    Number of LSAs: 0, checksum sum 0

```

Table 1-10 describes the significant fields shown in the display.

Table 1-10 ***show ip ospf Field Descriptions***

Field	Description
Routing Process...	OSPF instance tag and OSPF router ID.
Stateful High Availability	Status of stateful restart capability.
Graceful-restart	Status of graceful restart configuration.
grace period	Number of seconds that OSPF has to trigger a graceful restart.
Last graceful restart exit status	Exit status for last graceful restart.
Supports...	Number of types of service supported (Type 0 only).
Reference Bandwidth	Bandwidth used for cost calculation.
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum LSA arrival	Minimum interval between link-state advertisements.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>instance-tag</i>	(Optional) Name of the OSPF instance. Use this tag to display OSPF information about a specific OSPF instance. The <i>instance-tag</i> argument can be any alphanumeric string.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following example shows how to display information about border routers:

```
switch# show ip ospf border-routers

OSPF Process ID p1, vrf default Internal Routing Table
Codes: i - Intra-area route, I - Inter-area route

i 40.40.40.40 [10], ABR, Area 0.0.0.0, SPF 71 via
    192.0.2.1, Ethernet2/1
i 60.60.60.60 [20], ABR, Area 0.0.0.0, SPF 71 via
    192.0.2.1, Ethernet2/1
i 40.40.40.40 [10], ABR, Area 0.0.0.1, SPF 71 via
    192.0.2.1, Ethernet2/2
i 60.60.60.60 [20], ABR, Area 0.0.0.1, SPF 71 via
    192.0.2.1, Ethernet2/2
```

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-11 describes the significant fields shown in the display.

Table 1-11 ***show ip ospf border-routers Field Descriptions***

Field	Description
40.40.40.40	Router ID of the destination.
[10]	Cost of using this route.
ABR	Router type of the destination; the type is either an ABR, ASBR, or both.
Area	Area ID of the area from which this route is learned.
SPF 71	Internal number of the shortest path first (SPF) calculation that installs this route.
via 192.0.2.1	Next hop toward the destination.
Ethernet2/1	Interface type for the outgoing interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
<i>area-id</i>	(Optional) Area number used to define the particular area. Specify as either an IP address or a number from 0 to 4294967295.
<i>link-state-id</i>	(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 <i>ip-address</i>	(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.

Send document comments to nexus7k-docfeedback@cisco.com

external	(Optional) Displays information about the external LSAs.
ext_tag <i>value</i>	(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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to display the OSPF database:

```
Router# show ip ospf database
```

```
OSPF Router with ID (50.50.50.50) (Process ID p1)
```

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link Count
40.40.40.40	40.40.40.40	930	0x80000004	0x2ea1	3
50.50.50.50	50.50.50.50	935	0x80000002	0x8b52	1
60.60.60.60	60.60.60.60	943	0x800003c5	0x9854	2

Network Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
209.165.201.3	60.60.60.60	944	0x80000001	0x7179
192.0.2.1	50.50.50.50	935	0x80000001	0x516a

Summary Network Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
209.165.201.1	40.40.40.40	929	0x80000001	0x2498
209.165.201.1	50.50.50.50	928	0x80000001	0x5b2f
209.165.201.1	60.60.60.60	1265	0x800003c3	0xf49b
192.0.2.0	40.40.40.40	943	0x80000001	0x53f3
192.0.2.0	50.50.50.50	935	0x80000001	0x26f8
192.0.2.0	60.60.60.60	930	0x80000001	0x7b51

Table 1-12 describes the significant fields shown in the display.

Table 1-12 *show ip ospf database Field Descriptions*

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router's ID.
Age	Link state age.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	Checksum of the complete contents of the link state advertisement.
Link count	Number of interfaces detected for the router.

The following example shows how to display a summary of autonomous system border routers:

```
Router# show ip ospf database asbr-summary
```

```
OSPF Router with id(192.168.239.66) (Process ID 300)
```

Displaying Summary ASB Link States(Area 0.0.0.0)

```
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0 TOS: 0 Metric: 1
```

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-13 describes the significant fields shown in the display.

Table 1-13 *show ip ospf database asbr-summary Field Descriptions*

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (autonomous system boundary router).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	Checksum of the complete contents of the link state advertisement.
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link state metric.

The following example shows how to display information about external links:

```
Router# show ip ospf database external
```

```
OSPF Router with id(192.168.239.66) (Autonomous system 300)
```

```
        Displaying AS External Link States
```

```
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.105.0.0 (External Network Number)
Advertising Router: 172.16.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 1
    Forward Address: 0.0.0.0
    External Route Tag: 0
```

Table 1-14 describes the significant fields shown in the display.

Table 1-14 *show ip ospf database external Field Descriptions*

Field	Description
OSPF Router with id	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link state age.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-14 *show ip ospf database external Field Descriptions (continued)*

Field	Description
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (external network number).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	Checksum of the complete contents of the LSA.
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
Metric Type	External type.
TOS	Type of service.
Metric	Link state metric.
Forward Address	Forwarding address. Data traffic for the advertised destination will be forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
External Route Tag	External route tag; a 32-bit field attached to each external route. This field is not used by the OSPF protocol itself.

The following example shows how to display a summary of the OSPF database:

```
Router# show ip ospf database database-summary
```

```
OSPF Router with ID (100.0.0.1) (Process ID 1)
```

```
Area 0 database summary
```

LSA Type	Count	Delete	Maxage
Router	3	0	0
Network	0	0	0
Summary Net	0	0	0
Summary ASBR	0	0	0
Type-7 Ext	0	0	0
Self-originated Type-7	0		
Opaque Link	0	0	0
Opaque Area	0	0	0
Subtotal	3	0	0

```
Process 1 database summary
```

LSA Type	Count	Delete	Maxage
Router	3	0	0
Network	0	0	0
Summary Net	0	0	0
Summary ASBR	0	0	0
Type-7 Ext	0	0	0
Opaque Link	0	0	0
Opaque Area	0	0	0
Type-5 Ext	0	0	0
Self-originated Type-5	200		
Opaque AS	0	0	0
Total	203	0	0

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-15 describes the significant fields shown in the display.

Table 1-15 *show ip ospf database database-summary Field Descriptions*

Field	Description
Area 0 database summary	Area number.
Count	Count of LSAs of the type identified in the first column.
Router	Number of router link state advertisements in that area.
Network	Number of network link state advertisements in that area.
Summary Net	Number of summary link state advertisements in that area.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that area.
Type-7 Ext	Type-7 LSA count.
Self-originated Type-7	Self-originated Type-7 LSA.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count.
Subtotal	Sum of LSAs for that area.
Delete	Number of link state advertisements that are marked “Deleted” in that area.
Maxage	Number of link state advertisements that are marked “Maxaged” in that area.
Process 1 database summary	Database summary for the process.
Count	Count of LSAs of the type identified in the first column.
Router	Number of router link state advertisements in that process.
Network	Number of network link state advertisements in that process.
Summary Net	Number of summary link state advertisements in that process.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that process.
Type-7 Ext	Type-7 LSA count.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count.
Type-5 Ext	Type-5 LSA count.
Self-Originated Type-5	Self-originated Type-5 LSA count.
Opaque AS	Type-11 LSA count.
Total	Sum of LSAs for that process.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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*] [*interface-type interface-number*] [**brief**] [**vrf** *vrf-name*]

Syntax	Description
<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
<i>interface-type</i>	(Optional) Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
<i>interface-number</i>	(Optional) Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses, masks, and areas on the router.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples The following example shows how to display OSPF information for Ethernet interface 1/2:

```
switch# show ip ospf interface ethernet 1/2
Ethernet1/2 is up, line protocol is up
  IP address 192.0.2.1, Process ID 201 vrf default, area 10
```

Send document comments to nexus7k-docfeedback@cisco.com

```
State UP, Network type BROADCAST, cost 65535
Index 2, Transmit delay 1 sec, Router Priority 1
No designated router on this network
No backup designated router on this network
0 Neighbors, flooding to 0, adjacent with 0
Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
Simple authentication
Number of link LSAs: 0, checksum sum 0
```

Table 1-16 describes the significant fields shown in the display.

Table 1-16 ***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 of timer intervals.
Hello	Number of seconds until next hello packet is sent out this interface.

Send document comments to nexus7k-docfeedback@cisco.com

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 interface-type interface-number*

Syntax Description		
<i>neighbor id</i>		Router ID for the neighbor.
<i>interface-type</i>		(Optional) Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
<i>interface-number</i>		(Optional) Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command requires the Enterprise Services license.

Examples The following example shows how to display a list of LSAs that changed for Ethernet 2/1:

Router# **show ip ospf lsa-content-changed-list 192.0.2.2 ethernet 2/1**

[Table 1-18](#) describes the significant fields shown in the displays.

Table 1-17 *show ip ospf lsa-content-changed-list* Field Descriptions

Field	Description

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-17 *show ip ospf lsa-content-changed-list* Field Descriptions (continued)

Field	Description

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip ospf memory

To display the memory usage statistics for the Open Shortest Path First (OSPF) protocol, use the **show ip ospf memory** command.

show ip ospf memory

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	This command was removed.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to display the memory statistics for OSPF:

```
Router# show ip ospf memory
OSPF Process ID sd, Memory statistics
  Process memory: 2096 KB
  Byte usage:    needed 0, overhead 192, using 192 bytes
  Allocations:   current 6, created 6, failed 0, free 0
  Bitfields:     current 30, created 30, failed 0, free 0, using 248010 bytes
  Slabs:         current 2, created 2, failed 0, free 0, using 80 bytes
  Index failure: Interface 0, Neighbor 0

Slab Memory
OSPF vertex slab
Alloc 1, max allocs 1, total allocs 1, total frees 0
Total block allocs 1, total block frees 0, max blocks 1
Bytes (size/allocated) 68/69720
OSPF IPv4 prefix routes slab
Alloc 0, max allocs 0, total allocs 0, total frees 0
Total block allocs 0, total block frees 0, max blocks 0
Bytes (size/allocated) 188/64
OSPF router routes slab
Alloc 0, max allocs 0, total allocs 0, total frees 0
Total block allocs 0, total block frees 0, max blocks 0
Bytes (size/allocated) 100/64
```

Send document comments to nexus7k-docfeedback@cisco.com

```
OSPF IPv4 next-hops slab
Alloc 1, max allocs 1, total allocs 1, total frees 0
Total block allocs 1, total block frees 0, max blocks 1
Bytes (size/allocated) 32/262232
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip ospf neighbors

To display Open Shortest Path First (OSPF)-neighbor information on a per-interface basis, use the **show ip ospf neighbor** command.

show ip ospf [*instance-tag*] **neighbors** [*interface-type interface-number*] [*neighbor-id*] [**detail**] [**summary**] [**vrf** *vrf-name*]

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
<i>area-id</i>	(Optional) Area number used to define the particular area. Specify as an IP address or a number from 0 to 4294967295.
<i>interface-type</i>	(Optional) Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
<i>interface-number</i>	(Optional) Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.
<i>neighbor-id</i>	(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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to display the summary information about the neighbor that matches the neighbor ID:

```
Router# show ip ospf neighbors 10.199.199.137

Neighbor 10.199.199.137, interface address 192.0.2.37
  In the area 0.0.0.0 via interface Ethernet2/1
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:04
Neighbor 10.199.199.137, interface address 209.165.201.189
  In the area 0.0.0.0 via interface Ethernet4/3
  Neighbor priority is 5, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:03
```

The following example shows how to display the neighbors that match the neighbor ID on an interface:

```
Router# show ip ospf neighbors ethernet 2/1 10.199.199.137

Neighbor 10.199.199.137, interface address 192.0.2.37
  In the area 0.0.0.0 via interface Ethernet2/1
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:37
  Link State retransmission due in 0:00:04
```

The following example shows how to display detailed information about OSPF neighbors:

```
Router# show ip ospf neighbors detail

Neighbor 192.168.5.2, interface address 10.225.200.28
  In the area 0 via interface GigabitEthernet1/0/0
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.225.200.28 BDR is 10.225.200.30
  Options is 0x42
  LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
  Dead timer due in 00:00:36
  Neighbor is up for 00:09:46
Index 1/1, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 1, maximum is 1
Last retransmission scan time is 0 msec, maximum is 0 msec
```

Table 1-18 describes the significant fields shown in the displays.

Table 1-18 *show ip ospf neighbor detail Field Descriptions*

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor.
State	OSPF state.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-18 *show ip ospf neighbor detail Field Descriptions (continued)*

Field	Description
state changes	Number of state changes since the neighbor was created. This value can be reset using the clear ip ospf counters neighbor command.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates the area is not a stub; 0 indicates the area is a stub.)
LLS Options..., last OOB-Resync	Link-Local Signalling and out-of-band (OOB) link-state database resynchronization performed hours:minutes:seconds ago (NSF information). The field indicates the last successful out-of-band resynchronization with the NSF-capable router.
Dead timer due in	Expected time before Cisco NX-OS declares the neighbor dead.
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into a two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times that update packets have been resent during flooding.
First	First memory location of the flooding details.
Next	Next memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
	area <i>area-id</i>	Specifies the area number used to define the particular area. Specify as 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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following example shows how to display policy statistics for OSPF: switch# show ip ospf policy statistics area 201	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 | isis id | ospf
id | rip id | static } [vrf vrf-name]
```

Syntax	Description
<i>instance-tag</i>	(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).
isis	Displays policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
ospf	Displays policy statistics for OSPF.
rip	Displays policy statistics for the Routing Information Protocol (RIP).
static	Displays policy statistics for IP static routes.
<i>id</i>	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 autonomous system number. The range is from 1 to 65535. For the isis , 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Use the **show ip ospf policy statistics redistribute** command to display redistribution statistics. This command requires the Enterprise Services license.

Examples

The following example shows how to display policy statistics for redistributed routes:

```
switch# show ip ospf policy statistics redistribute
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 interface interface-number*

Syntax Description		
<i>neighbor-id</i>		Router ID of the neighbor. Specify as an IP address.
<i>interface-type</i>		Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
<i>interface-number</i>		Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples

The following example shows how to display a list of all LSAs requested by a router:

```
Router# show ip ospf request-list 40.40.40 ethernet 2/1
OSPF Process ID p1
Neighbor 40.40.40.40, interface Ethernet2/1, address 192.0.2.1
1 LSAs on request-list

Type  LS ID          ADV RTR          Seq NO          Age          Checksum
1   192.0.2.12       192.0.2.12       0x8000020D      8            0x6572
```

Table 1-19 describes the significant fields shown in the displays.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-19 *show ip ospf request-list Field Descriptions*

Field	Description
Type	LSA type.
LS ID	IP address of the neighbor router.
ADV RTR	IP address of the advertising router.
Seq NO	Packet sequence number of the LSA.
Age	Age, in seconds, of the LSA.
Checksum	Checksum number of the LSA.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 interface interface-number*

Syntax Description	<i>neighbor-id</i>	Router ID of the neighbor. Specify as an IP address.
	<i>interface-type</i>	Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
	<i>interface-number</i>	Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples The following example shows how to display all LSAs waiting to be resent to neighbors:

```
Router# show ip ospf retransmission-list 192.0.2.11 ethernet 2/1

      OSPF Router with ID (192.0.2.12) (Process ID 1)

Neighbor 192.0.2.11, interface Ethernet2/1 address 209.165.201.11
Link state retransmission due in 3764 msec, Queue length 2

Type  LS ID          ADV RTR          Seq NO          Age          Checksum
  1   192.0.2.12      192.0.2.12      0x80000210      0            0xB196
```

Table 1-20 describes the significant fields shown in the displays.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-20 ***show ip ospf retransmission-list Field Descriptions***

Field	Description
Type	LSA type.
LS ID	IP address of the neighbor router.
ADV RTR	IP address of the advertising router.
Seq NO	Packet sequence number of the LSA.
Age	Age, in seconds, of the LSA.
Checksum	Checksum number of the LSA.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip ospf routes

To display the Open Shortest Path First (OSPF) topology table, use the **show ip ospf routes** command.

show ospf [*instance-tag*] **routes** [*prefix/length* | **summary**] [**vrf** *vrf-name*]

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
<i>prefix /length</i>	(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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples

The following example shows how to display OSPF routes:

```
RP/0/RP0/CPU0:router# show ip ospf routes
OSPF Process ID sd vrf default, Routing Table
(D) denotes route is directly attached      (R) denotes route is in RIB
61.61.61.61/32 (i) area 1
    via 192.168.2.1/Ethernet2/2, cost 21
100.100.2.0/24 (i) area 1
    via 192.168.2.1/Ethernet2/22, cost 20
```

Send document comments to nexus7k-docfeedback@cisco.com

```
192.168.2.0/24 (i) area 1  
    via directly connected
```

Table 1-21 describes the significant fields shown in the display.

Table 1-21 *show ospf route Field Descriptions*

Field	Description
61.61.61.61/32	Router ID for the router that advertised this route.
via...	Packets destined for the given prefix are sent over the listed interface or directly connected to this device.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string up to 20 characters.
vrf <i>vrf-name</i>	(Optional) Name of the VRF. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following example shows how to display information about the SPF calculations:

```
Router# show ip ospf statistics
OSPF Process pl vrf default, Event statistics (cleared 2w3d ago)
  Router ID changes: 0
  DR elections: 50
  Older LSAs received: 16
  Neighbor state changes: 82
  Neighbor dead postponed: 0
  Neighbor dead interval expirations: 2
  Neighbor bad lsreqs: 0
  Neighbor sequence number mismatches: 0
  SPF computations: 101 full, 23 summary, 23 external
```

Send document comments to nexus7k-docfeedback@cisco.com

LSA Type	Generated	Refreshed	Flushed	Aged out
Router	41	1678	4	3
Network	12	2	15	1
Summary Net	53	6	120	6
Summary ASBR	0	0	0	0
AS External	0	0	0	0
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, 14 hwm, 183 deleted, 14 revived, 27 runs
 Hello queue: 0/200, hwm 2, drops 0
 Flood queue: 0/100, hwm 2, drops 0
 LSDB additions failed: 0

Buffers:	in use	hwm	permanent	alloc	free
128 bytes	0	2	2	350300	350300
512 bytes	0	2	2	114	114
1520 bytes	0	0	0	0	0
4500 bytes	0	1	1	355	355
huge	0	0	0	0	0

Table 1-22 describes the significant fields shown in the display.

Table 1-22 *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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	
<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to display information about summary addresses:

```
Router# show ip ospf summary-address
```

```
OSPF Process 2, Summary-address
```

```
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

[Table 1-18](#) describes the significant fields shown in the displays.

Table 1-23 *show ip ospf summary-address* Field Descriptions

Field	Description
10.2.0.0/255.255.0.0	IP address and mask of the router for the OSPF process.
Metric -1	OSPF metric type.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-23 *show ip ospf summary-address* Field Descriptions (continued)

Field	Description
Type 0	Type of LSA.
Tag 0	OSPF process tag identifier.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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** [*vrf vrf-name*]

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following example shows how to display OSPF traffic statistics:

```
Router# show ip ospf traffic
```

```
OSPF Process ID p1, vrf Red, Packet Counters (cleared 2w3d ago)
Total: 1690 in, 349230 out
LSU transmissions: first 100, rxmit 108, for req 16
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, 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, nbr changed rid/ip addr 0
       bad auth      0
       hellos        dbds      lsreqs      lsus        acks
```


Send document comments to nexus7k-docfeedback@cisco.com

```

In:          1411          70          16          136          57
Out:         348871        62           4          224          69

```

Table 1-24 describes the significant fields shown in the display.

Table 1-24 ***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.
Errors	
drops	Number of packets dropped.
bad version	Number of packets received with bad version.
dup rid	Number of packets with a duplicate router-id
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)
lsacks	Number of packets of type LSACK (LSA acknowledged)

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPF traffic statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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
<i>instance-tag</i>	(Optional) Instance tag. Specify as an alphanumeric string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
<i>instance-tag</i>	(Optional) Instance tag. Use this tag to display OSPF information about a specific OSPF instance.
brief	(Optional) Displays a summary of the configured virtual links.
vrf <i>vrf-name</i>	(Optional) Name of the OSPF VRF. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings “default” and “all” are reserved <i>vrf-names</i> .

Defaults None

Command Modes Any

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples The following example shows how to display information about virtual links:

```
Router# show ip ospf virtual-links
```

```
Virtual link 2 to router 40.40.40.40 is up
  Process ID p1 vrf default, Transit area 1, via interface Ethernet1/2, cost 10
  Local Address 192.0.2.2, Remote Address 192.0.2.1
  Index 4, Transmit delay 1 sec
  1 Neighbors, flooding to 1, adjacent with 1
  Timer intervals: hello 10, dead 40, wait 40, retransmit 5
  Hello timer due in 00:00:04
```

Send document comments to nexus7k-docfeedback@cisco.com

```
No authentication
Number of link LSAs: 0, checksum sum 0
Neighbor State is FULL, 4 state changes, last change 00:00:03
Hello options 0x2, dbd options 0x42
Last non-hello packet received 00:00:01
Dead timer due in 00:00:36
```

Table 1-25 describes the significant fields shown in the display.

Table 1-25 *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 timer due in 0:00:04	Time when the next hello is expected from the neighbor.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip policy

To display the route policy information, use the **show ip policy** command.

show ip policy [*vrf vrf-name*]

Syntax Description	<i>vrf vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows the policies attached to interfaces:

```
switch(config-if)# show ip policy
Interface      Route-map      Status      VRF-Name
Ethernet2/45   floor1         Inactive    --
```

Related Commands	Command	Description
	ip policy	Configures a route policy on an interface.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>name</i> (Optional)Name of community list. The name can be any case-sensitive alphanumeric string up to 63 characters.				
Defaults	None				
Command Modes	Any command mode				
Supported User Roles	network-admin network-operator vdc-admin vdc-operator				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
Usage Guidelines	This command does not require a license.				
Examples	This example displays the prefix lists: <pre>switch(config)# show ip prefix-list ip prefix-list test2: 1 entries seq 5 permit 10.0.0.0/8</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip prefix-list</td><td>Configures a BGP prefix list.</td></tr></table>	Command	Description	ip prefix-list	Configures a BGP prefix list.
Command	Description				
ip prefix-list	Configures a BGP prefix list.				

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip process

To display formation about the IP process, use the **show ip process** command.

show ip process [*vrf vrf-name*]

Syntax Description	<i>vrf vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows details on 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: 80
  Local address list:
```

Related Commands	Command	Description
	show ipv6 process	Displays information about the IPv6 process.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>instance-tag</i>	(Optional) Selects a RIP instance.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	No default behavior or values

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example is sample output from the show ip rip command:

```
switch(config-if)# show ip rip
Process Name "rip-sd" vrf "default"
RIP port 520, multicast-group 224.0.0.9
Admin-distance: 40
Updates every 30 sec, expire in 180 sec
Collect garbage in 120 sec
Default-metric: 1
Max-paths: 8
Process is up and running
  Interfaces supported by ipv4 RIP :
    Ethernet1/2
```

[Table 1-26](#) describes the significant fields shown in the display.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-26 *show ip rip Field Descriptions*

Field	Description
Process Name	The RIP instance tag.
Admin-distance	The administrative distance assigned to RIP. You can configure this value using the distance command in router address-family configuration mode.
Updates	Timer value for RIP updates. Configure this value with the ip rip timer basic command in interface configuration mode.
expire	Timer value for expiring RIP updates. Configure this value with the ip rip timer basic command in interface configuration mode.
Collect garbage	Timer value for garbage collecting in the RIP route table. Configure this value with the ip rip timer basic command in interface configuration mode.
Default metric	Default metric value. Configure this value with the default-metric command in router address-family mode.
Max-paths	Number of maximum paths allowed per RIP route. Configure this value with the max-paths command in router address-family mode.
Process	Administrative and operational state of this RIP instance.
Interfaces supported	RIP version and list of interfaces configured for this RIP instance. Add or remove interfaces using the ip router rip command in interface configuration mode.

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.

Send document comments to nexus7k-docfeedback@cisco.com

show ip rip interface

To display interface entry information from the the Routing Information Protocol (RIP) topology table, use the **show ip rip interface** command in any mode.

show ip rip interface [*type instance*] [**vrf** *vrf-name*]

Syntax Description

interface <i>type slot/port</i>	(Optional) Specifies the interface.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

This command has no default settings.

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example is sample output from the **show ip rip interface** command:

```
switch(config-if)# show ip rip interface ethernet 1/2
Process Name "rip-sd" vrf "default"
RIP-configured interface information
```

```
GigabitEthernet1/2, protocol-down/link-down/admin-down, RIP state : down
address/mask NotConfigured, metric 1, split-horizon
```

[Table 1-27](#) describes the significant fields shown in the display.

Table 1-27 show ip rip interface Field Descriptions

Field	Description
Process Name	RIP instance tag.
vrf	Virtual routing and forwarding (VRF) of this interface.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-27 *show ip rip interface Field Descriptions (continued)*

Field	Description
Interface information	Interface administrative and operational state.
RIP state	RIP information for this interface.

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip rip neighbor

To display the neighbor information from the 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	<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	No default behavior or values

Command Modes	Any

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following is sample output from the show ip rip neighbor command:

```
switch(config-if)# show ip rip neighbor
Process Name "rip-sd" vrf "default"
RIP Neighbor Information (number of neighbors = 0)
('dead' means more than 300 seconds ago)
```

[Table 1-28](#) describes the significant fields shown in the display.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-28 *show ip rip neighbor* Field Descriptions

Field	Description
Process Name	RIP instance tag.
vrf	Virtual routing and forwarding (VRF) of this interface.
Neighbor information	Number of RIP neighbors recognized on this interface.

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 | isis id | ospf id | ospfv3 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).
isis	Displays policy statistics for Intermediate-System to Intermediate-System (IS-IS) routing protocol.
ospf	Displays policy statistics for Open Shortest Path First (OSPF) protocol.
ospfv3	Displays policy statistics for Open Shortest Path First version 3 (OSPFv3) protocol.
static	Displays policy statistics for IP static routes.
<i>id</i>	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 NX-OS stores it internally as a string. For the isis keyword, an IS-IS 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 NX-OS 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 NX-OS stores it internally as a string.
vrf vrf-name	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults No default behavior or values.

Command Modes Any

Supported User Roles network-admin
vdc-admin

Send document comments to nexus7k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to show policy statistics for EIGRP:

```
switch# show ip rip policy statistics redistribute eigrp 201
```

Related Commands**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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip rip route

To display route information from the 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	<i>prefix/length</i>	(Optional) IP or IPv6 prefix about which routing information should be displayed.
	summary	(Optional) Displays information about summary routes.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	No default behavior or values

Command Modes	Any

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following is sample output from the show ip rip route command:

```
:switch# show ip rip route
```

[Table 1-28](#) describes the significant fields shown in the display.

Table 1-29 *show ip rip route* Field Descriptions

Field	Description

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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
show ip rip policy statistics	Displays policy statistics for RIP.
show ip rip statistics	Displays RIP statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip rip statistics

To display statistical entry information from the 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	<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive 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 History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example is sample output from the show ip rip statistics command:

```
switch# show ip rip statistics
Global update stats:
  Sent Multicast Updates: periodic 0,triggered 0
  Sent Multicast Requests: 0
  Sent Unicast Updates: 544
  Sent Unicast Requests: 544
  Recv Multicast Updates: 0
  Recv Multicast Requests: 0
  Recv Unicast Updates: 500
  Recv Unicast Requests: 544
  Recv Bad Pkts: 0
  Recv Bad Routes: 0
```

[Table 1-30](#) describes the significant fields shown in the display.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-30 ***show rip statistics Field Descriptions***

Field	Description
Sent Multicast Updates:	Number of RIP multicast updates sent.
Sent Multicast Requests:	Number of RIP multicast requests sent.
Sent Unicast Updates:	Number of RIP unicast updates sent.
Sent Unicast Requests:	Number of RIP unicast requests sent.
Recv Multicast Updates:	Number of RIP multicast updates received.
Recv Multicast Requests:	Number of RIP multicast requests received.
Recv Unicast Updates:	Number of RIP unicast updates received.
Recv Unicast Requests:	Number of RIP unicast requests received.
Recv Bad Pkts:	Number of bad RIP packets received.
Recv Bad Routes:	Number of bad RIP routes received.

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.

Send document comments to nexus7k-docfeedback@cisco.com

show ip route

To display routes from the unicast 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.
	<i>addr</i>	(Optional) IPv4 address. The format is x.x.x.x.
	<i>hostname</i>	Host name. The <i>name</i> can be any case-sensitive alphanumeric string up to 80 characters.
	<i>prefix</i>	(Optional) IPv4 prefix. The format is x.x.x.x/length. The length range is from 1 to 32.
	<i>route-type</i>	(Optional) Type of route. Use ? to see the list of types.
	interface <i>type number</i>	(Optional) Displays the routes for an interface. Use ? to see the supported interfaces.
	next-hop <i>addr</i>	(Optional) Displays routes with this next-hop address. The format is x.x.x.x.
	vrf <i>vrf-name</i>	(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

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(3)	This command was introduced.
	4.1(2)	Added <i>hostname</i> argument.

Usage Guidelines	This command does not require a license.

Examples	This example displays the route table: <pre>switch(config)# show ip route all IP Route Table for VRF "default" '*' denotes best ucast next-hop '*' denotes best mcast next-hop '[x/y]' denotes [preference/metric]</pre>

Send document comments to nexus7k-docfeedback@cisco.com

```
0.0.0.0/32, 1 ucast next-hops, 0 mcast next-hops
  *via Null0, [220/0], 00:45:24, local, discard
255.255.255.255/32, 1 ucast next-hops, 0 mcast next-hops
  *via sup-eth1, [0/0], 00:45:24, local
```

Related Commands

Command	Description
clear ip route	Clears entries in the route table.

Send document comments to nexus7k-docfeedback@cisco.com

show ip static-route

To display static routes from the unicast RIB, use the **show ip static-route** command.

show ip static-route [**vrf** {*vrf-name* | **all**}]

Syntax Description	vrf <i>vrf-name</i>	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
	all	(Optional) Specifies all virtual router contexts (VRF) name.
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.2(1)	Added all keyword.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the static routes:	
	<pre>switch(config)# show ip static-route IPv4 Unicast Static Routes: Total number of routes: 0, unresolved: 0</pre>	
Related Commands	Command	Description
	ip route	Configures a static route.

Send document comments to nexus7k-docfeedback@cisco.com

show ip traffic

To display IP traffic information, use the **show ip traffic** command.

show ip traffic

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the IP traffic information:

```
switch(config)# show ip traffic

IP Software Processed Traffic Statistics
-----
Transmission and reception:
  Packets received: 14121, sent: 3415, consumed: 0,
  Forwarded, unicast: 0, multicast: 0, Label: 0
Opts:
  end: 0, nop: 0, basic security: 0, loose source route: 0
  timestamp: 0, extended security: 0, record route: 0
  stream ID: 0, strict source route: 0, alert: 45, cipso: 0, ump: 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: 126, no buffer dropped: 0,
  Bad encapsulation: 0, no route: 0, non-existent protocol: 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
```

Send document comments to nexus7k-docfeedback@cisco.com

ICMP Software Processed Traffic Statistics

Transmission:

Redirect: 0, unreachable: 0, echo request: 0, echo reply: 1,
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: 0, unreachable: 337, echo request: 1, 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,
Format error: 0, checksum error: 0

Statistics last reset: never

Related Commands

Command	Description
show ip process	Displays information about the IP process.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ip wccp

To display global statistics that are related to the Web Cache Communication Protocol (WCCP), use the **show ip wccp** command.

show ip wccp [**vrf** *vrf-name*] [*service-number* | **web-cache**] [**detail** | **mask** | **service** | **view**]

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies the VRF in which the service group needs to be created. If no VRF is specified, then the service number is created in the default global VRF. The <i>vrf-name</i> can be any case-sensitive alphanumeric string up to 32 characters.
<i>service-number</i>	(Optional) Dynamic service identifier. The <i>service-number</i> range is from 1 to 255.
web-cache	(Optional) Displays information about the web-cache well-known service.
detail	(Optional) Displays information about the device and all web caches.
mask	(Optional) Displays information about the WCCP mask.
service	(Optional) Displays information about the WCCP service.
view	(Optional) Displays information about the members of a service group that have or have not been detected.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **show ip wccp** *service-number* command to provide the Total Packets Redirected count. The Total Packets Redirected count is the number of flows, or sessions, that are redirected.

Use the **show ip wccp** *service-number* **detail** command to provide the Packets Redirected count. The Packets Redirected count is the number of flows, or sessions, that are redirected.

Use the **clear ip wccp** command to reset the statistics.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to display the WCCP information for service 90:

```
switch(config)# show ip wccp 90
Service Identifier: 90
  Number of Service Group Clients:      1
  Number of Service Group Routers:     1
  Total Packets Redirected:             0
  Service mode:                        Closed
  Service Access-list:                  tcp91
  Total Packets Dropped Closed:         0
  Redirect Access-list:                 -none-
  Total Packets Denied Redirect:        0
  Total Packets Unassigned:             0
  Total Authentication failures:        0
  Total Bypassed Packets Received:      0
```

Table 1-31 describes the significant fields shown in the display.

Table 1-31 ***show ip wccp Field Descriptions***

Field	Description
Service Identifier	Service that is detailed.
Number of Service Group Clients	Number of routers in the service group.
Total Packets Redirected	Total number of packets redirected by the router.
Service mode	WCCP service mode. Options are open or closed.
Service Access-list	Named IP access list that defines the packets that match the service.
Total Packets Dropped Closed	Total number of packets that are dropped when WCCP is configured for closed services and an intermediary device is not available to process the service.
Redirect Access-list	Name of the access list that determines which packets are redirected.
Total Packets Denied Redirect	Total number of packets that are not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that are not redirected because they are not assigned to any cache engine. Packets may not be assigned during the initial discovery of cache engines or when a cache is dropped from a cluster.
Total Authentication failures	Number of instances where a password did not match.
Total Bypassed Packets Received	Number of packets that are bypassed (coming in through the negotiated return method).

The following example shows how to display the WCCP group member details for service 10:

```
switch(config)# show ip wccp 10 view

WCCP Router Informed of:
  10.168.88.10
  10.168.88.20

WCCP Cache Engines Visible
  10.168.88.11
  10.168.88.12
```

Send document comments to nexus7k-docfeedback@cisco.com

```
WCCP Cache Engines Not Visible:
-none-
```

If any cache engine is displayed under the WCCP Cache Engines Not Visible field, the router needs to be reconfigured to map the cache engine that is not visible to it.

Table 1-32 describes the significant fields shown in the display.

Table 1-32 *show ip wccp view Field Descriptions*

Field	Description
WCCP Router Informed of	List of routers detected by the current router.
WCCP Clients Visible	List of clients that is visible to the router and other clients in the service group.
WCCP Clients Not Visible	List of clients in the service group that is not visible to the router and other clients in the service group.

The following example shows how to display the WCCP client information and WCCP router statistics that include the type of services:

```
switch(config)# show ip wccp 91 detail
WCCP Client information:

WCCP Client ID:      10.1.1.1
Protocol Version:    2.0
State:               Usable (Usable)
Redirection:         L2
Packet Return:       L2
Packets Redirected:  0
Connect Time:        00:01:15
Assignment:          MASK
Bypassed Packets:    0
Mask  SrcAddr  DstAddr  SrcPort  DstPort
----  -
0001: 0x00000001 0x00000000 0x0000  0x0000
Value SrcAddr  DstAddr  SrcPort  DstPort CE-IP
-----
0001: 0x00000000 0x00000000 0x0000  0x0000  0x0a010101 (10.1.1.1)
0002: 0x00000001 0x00000000 0x0000  0x0000  0x0a010101 (10.1.1.1)
```

Table 1-33 describes the significant fields shown in the display.

Table 1-33 *show ip wccp detail Field Descriptions*

Field	Description
WCCP Router information	Header for the area that contains fields for the IP address and version of WCCP associated with the router connected to the cache engine in the service group.
IP Address	IP address of the router connected to the cache engine in the service group.
WCCP Client Information	Header for the area that contains fields for information on clients.
IP Address	IP address of the cache engine in the service group.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-33 *show ip wccp detail Field Descriptions (continued)*

Field	Description
State	Whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Packets Redirected	Number of packets that are redirected to the cache engine.
Connect Time	Amount of time that the cache engine is connected to the router.
Bypassed Packets	Number of packets that are bypassed.

Related Commands

Command	Description
clear ip wccp	Clears the counter for packets redirected by WCCP.
ip wccp	Enables WCCP on a router and specifies the type of services to be used.
show ip interface	Lists a summary of the IP information and status of an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 adjacency

To display adjacency information, use the **show ipv6 adjacency** command.

show ipv6 adjacency [*ipv6-addr* | *interface*] [**detail**] [**non-best**] [**statistics**] [**summary**] [**vrf** *vrf-name*]

Syntax Description

<i>ipv6-addr</i>	(Optional) An IPv6 source address. The format is A:B::C:D
<i>interface</i>	(Optional) An interface. Use ? to determine the supported interface types.
detail	(Optional) Displays detailed adjacency information.
non-best	(Optional) Displays the best adjacency entries and the alternate adjacency entries.
statistics	(Optional) Displays adjacency statistics.
summary	(Optional) Displays a summary of the adjacency information.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Added non-best and summary keywords.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays a summary of the adjacency information:

```
switch# show ipv6 adjacency summary
IPv6 Adjacency Table for VRF default
Total number of entries: 0
Address          Age          MAC Address      Pref Source      Interface
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
show forwarding adjacency	Displays forwarding adjacency information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp

To display entries in the Border Gateway Protocol (BGP) table, use the **show ipv6 bgp** command.

```
show ipv6 bgp [ipv6-addr | ipv6-prefix [longer-prefixes]] [received-paths] [regex expression]
[route-map map-name] [summary] [vrf vrf-name]
```

Syntax Description

<i>ipv6-addr</i>	(Optional) A network from the BGP route table. The format is A:B::C:D.
<i>ipv6-prefix</i>	(Optional) A prefix from the the BGP route table. The format is A:B::C:D/length.
longer-prefixes	(Optional) Displays the prefix and any more specific routes.
received-paths	(Optional) Displays paths stored for soft reconfiguration.
regex <i>expression</i>	(Optional) Display information that matches the regular expression.
route-map <i>map-name</i>	(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 <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the BGP route table:

```
switch(config-router)# show ipv6 bgp
BGP routing table information for VRF default, address family IPv6 Unicast
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
clear bgp	Clears entries in the BGP route table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp community

To display Border Gateway Protocol (MP-BGP) routes that match a community, use the **show ipv6 bgp community** command.

```
show ipv6 bgp community [as-number] [internet] [no-advertise] [no-export]
[no-export-subconfed] [exact-match]} [vrf vrf-name]
```

Syntax Description

<i>as-number</i>	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>.
internet	(Optional) Displays the internet community.
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.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays routes that match a community:

```
switch(config)# show ipv6 bgp community
```

Related Commands

Command	Description
ip community-list	Creates a community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp community-list

To display Border Gateway Protocol (BGP) routes that match a community list, use the **show ipv6 bgp community-list** command.

```
show ipv6 bgp [community-list commlist-name [exact-match]] [vrf vrf-name]
```

Syntax Description	community-list <i>commlist-name</i>	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.
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays routes that match a community list: switch(config)# show ipv6 bgp community-list test1	
Related Commands	Command	Description
	ip community-list	Creates a community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp dampening

To display Border Gateway Protocol (BGP) dampening information, use the **show ipv6 bgp dampening** command.

show ipv6 bgp dampening { **dampened-paths** [**regex** *expression*] | **flap-statistics** | **history-paths** [**regex** *expression*] | **parameters** } [**vrf** *vrf-name*]

Syntax Description

dampened-paths	Display all dampened paths.
regex <i>expression</i>	(Optional) Display information that matches the regular expression.
flap-statistics	Display flap statistics for routes.
history-paths	Display all history paths.
parameters	Display all dampening parameters.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays dampening information:

```
switch(config)# show ipv6 bgp dampening dampened-paths
```

Related Commands

Command	Description
show ip bgp dampening	Displays BGP dampening information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp extcommunity-list

To display Border Gateway Protocol (BGP) routes that match an extended community list, use the **show ipv6 bgp extcommunity-list** command.

show ipv6 bgp extcommunity-list *commlist-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description	<i>commlist-name</i>	Name of an extended community-list. The <i>commlist-name</i> can be any case-sensitive alphanumeric string up to 63 characters.
	exact-match	(Optional) Displays an exact match of the extended communities.
	vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a community list: switch(config)# show ipv6 bgp extcommunity-list test1

Related Commands	Command	Description
	ip extcommunity-list	Creates an extended community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp filter-list

To display Border Gateway Protocol (BGP) routes that match a filter list, use the **show ipv6 bgp filter-list** command.

show ipv6 bgp filter-list *list-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description	<i>list-name</i>	Name of a filter-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 <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a filter list: switch(config)# show ipv6 bgp filter-list test1

Related Commands	Command	Description
	show ip bgp filter-list	Displays BGP routes that match a filter list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp flap-statistics

To display Border Gateway Protocol (BGP) flap statistics, use the **show ipv6 bgp flap-statistics** command.

show ipv6 bgp flap-statistics [*prefix*] [**vrf** *vrf-name*]

Syntax Description	<i>prefix</i>	(Optional) IPv6 prefix. The format is A:B::C:D/length.
	vrf <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the flap statistics: switch(config)# show ipv6 bgp flap-statistics	
Related Commands	Command	Description
	show ip bgp	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp history-paths

To display Border Gateway Protocol (BGP) history paths, use the **show ipv6 bgp history-paths** command.

show ipv6 bgp history-paths [**regexp** *expression*] [**vrf** *vrf-name*]

Syntax Description	regexp <i>expression</i>	(Optional) Display information that matches the regular expression.
	vrf <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays BGP history path information:	
	switch(config)# show ipv6 bgp history-paths	
Related Commands	Command	Description
	show ip bgp history-paths	Displays BGP history paths information.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 bgp neighbors

To display Border Gateway Protocol (BGP) neighbors, use the **show ipv6 bgp neighbors** command.

```
show ipv6 bgp neighbors [ addr [advertised-routes | flap-statistics | paths | received-routes |  
routes [advertised | dampened | received]] | prefix] [vrf { all | vrf-name }]
```

Syntax Description	
<i>addr</i>	IPv6 address. The format is A:B::C:D.
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.
<i>prefix</i>	(Optional) IPv6 prefix. The format is A:B::C:D/length.
vrf <i>vrf-name</i>	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
all	(Optional) Specifies all VRFS.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added paths keyword.

Usage Guidelines	This command does not require a license.

Examples	This example displays the BGP neighbors:

 `show ipv6 bgp neighbors`

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# show ipv6 bgp neighbors
```

Related Commands

Command	Description
<code>show ip bgp neighbors</code>	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 bgp nexthop

To display Border Gateway Protocol (BGP) next hop information, use the **show ipv6 bgp nexthop** command.

show ipv6 bgp nexthop *addr* [**vrf** *vrf-name*]

Syntax Description	<i>addr</i>	IPv4 address. The format is A:B::C:D.
	vrf <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the BGP next-hop information: switch(config)# show ipv6 bgp nexthop 2001:0DB8::1	
Related Commands	Command	Description
	show ip bgp nexhop	Displays BGP information.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 bgp nexthop-database

To display Border Gateway Protocol (BGP) next-hop database, use the **show ipv6 bgp nexthop-database** command.

show ipv6 bgp nexthop-database [**vrf** *vrf-name*]

Syntax Description

vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the BGP next-hop database:

```
switch(config)# show ipv6 bgp nexthop-database
```

Related Commands

Command	Description
show ip bgp nexthop-database	Displays BGP information.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 bgp prefix-list

To display Border Gateway Protocol (BGP) routes that match a prefix list, use the **show ipv6 bgp prefix-list** command.

```
show ipv6 bgp prefix-list list-name [exact-match] [vrf vrf-name]
```

Syntax Description	<i>list-name</i>	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 <i>vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays routes that match a prefix list: <pre>switch(config)# show ipv6 bgp prefix-list test1</pre>	
Related Commands	Command	Description
	show ip bgp prefix-list	Displays BGP routes that match a prefix list.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 client

To display information about the internal IPv6 clients, use the **show ipv6 client** command.

show ipv6 client [*name*]

Syntax Description	<i>name</i> (Optional) Name of client.	
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the IPv6 client information for ICMPv6: <pre>switch(config-if)# show ipv6 client icmpv6 IPv6 Registered Client Status Client: icmpv6, status: up, pid: 3688, extended pid: 3688 Protocol: 58, pib-index: 2, routing context id: 255 Control mts SAP: 1551 Data mts SAP: 1552 IPC messages to control mq: 3 IPC messages to data mq: 0</pre>	
Related Commands	Command	Description
	show ipv6 process	Displays information about the IPv6 process.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 eigrp

To display a summary of the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 processes, use the **show ipv6 eigrp** command.

show ipv6 eigrp [*instance-tag*]

Syntax Description	<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to display all the EIGRP for IPv6 instances:

```
switch# show ipv6 eigrp
IP-EIGRP AS 0 ID 0.0.0.0 VRF default
  Process-tag: Test1
  Status: shutdown
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  IP proto: 88 Multicast group: ff02::000a
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Number of EIGRP interfaces: 0 (0 loopbacks)
  Number of EIGRP peers: 0
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 eigrp accounting

To display prefix accounting information for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 processes, use the **show ipv6 eigrp accounting** command.

show ipv6 eigrp [*instance-tag*] **accounting** [**vrf** {*vrf-name* | *}]

Syntax Description

<i>instance-tag</i>	(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 63 characters.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the EIGRP accounting information:

```
switch# show ipv6 eigrp accounting
```

```
IPv6-EIGRP accounting for AS(100)/ID(192.0.2.1) vrf RED
Total Prefix Count: 4
States: A-Adjacency, P-Pending, D-Down
```

State	Address/Source	Interface	Prefix Count	Restart Count	Restart/Reset (s)
P	Redistributed	----	0	3	211
A	2001:0DB8::2	e2/1	2	0	84
P	2001:0DB8::3	e3/3	0	2	114
D	2001:0DB8::4	e4/1	0	3	0

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-4 describes the significant fields shown in the display.

Table 1-34 *show ipv6 eigrp accounting Field Descriptions*

Field	Description
IPv6-EIGRP accounting for AS...	EIGRP instance, AS number, router ID, and table ID.
Total Prefix Count:	Aggregate sum of the prefixes in an EIGRP instance topology table. The count includes prefixes learned from all neighbors or from redistribution.
States: A-Adjacency, P-Pending, D-Down	A-Adjacency—Indicates a stable adjacency with the neighbor or a normal redistribution state. P-Pending—Neighbor adjacency or redistribution is suspended or in a penalized state because the maximum prefix limit was exceeded. D-Down—Neighbor adjacency or redistribution is suspended permanently until a manual reset is performed with the clear route command.
Address/Source	Peer IP address of the redistribution source.
Prefix Count	Total number of learned prefixes by source. Note Routes can be learned for the same prefix from multiple sources, and the sum of all prefix counts in this column may be greater than the figure displayed in the “Prefix Count” field.
Restart Count	Number of times that a route source exceeded the maximum prefix limit.
Restart Reset(s)	Time, in seconds, that a route source is in a P (penalized) state. If the route source is in an A (stable or normal) state, the displayed time, in seconds, is the time period until penalization history is reset.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 eigrp interfaces

To display information about interfaces configured for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp interfaces** command.

show ipv6 eigrp [*instance-tag*] **interfaces** [*type instance*] [**brief**] [**vrf** {*vrf-name* | *}]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
vrf *	(Optional) Specifies all VRF instances.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance. Specifying <i>instance</i> removes all entries learned through this interface from the neighbor table. For more information, use the question mark (?) online help function.
brief	(Optional) Displays a brief summary of EIGRP interface information.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

This command shows all interfaces for the default VRF if no VRF or interface is specified.

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **show ipv6 eigrp interfaces** command to determine on which interfaces EIGRP is active and to 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.

Send document comments to nexus7k-docfeedback@cisco.com

This command requires the Enterprise Services license.

Examples

The following example shows how to display information about EIGRP interfaces:

```
switch# show ipv6 eigrp interfaces brief
```

```
IPv6 EIGRP interfaces for process 1 vrf default
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
e2/2	0	0/0	0	11/434	0	0
e2/20	1	0/0	337	0/10	0	0
e4/2	1	0/0	10	1/63	103	0
e3/2	1	0/0	330	0/16	0	0

```
switch#
```

[Table 1-5](#) describes the significant fields shown in the display.

Table 1-35 *show ip eigrp interfaces Field Descriptions*

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.
Xmit Queue Un/Reliable	Number of packets remaining in the unreliable and reliable transmit queues.
Mean SRTT	Mean smoothed round-trip time (SRTT) internal (in milliseconds).
Pacing Time Un/Reliable	Pacing time used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the router sends multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.

Related Commands

Command	Description
show ipv6 eigrp neighbors	Displays the neighbors discovered by EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 eigrp neighbors

To display information about neighbors discovered by the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp neighbors** command.

show ipv6 eigrp [*instance-tag*] **neighbors** [**detail**] [*interface-type interface-instance*] [**static**] [**vrf** {*vrf-name* | *}]

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
vrf *	(Optional) Specifies all VRF instances.
detail	(Optional) Displays detailed EIGRP neighbor information.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance. Specifying <i>instance</i> removes all entries learned through this interface from the neighbor table. For more information about the syntax for the router, use the question mark (?) online help function.
static	(Optional) Displays static EIGRP interface information.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults This command displays all neighbors for the default VRF on all interfaces if no VRF or interface is specified.

Command Modes Any

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines Use the **show ipv6 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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to display information about EIGRP neighbors:

```
switch# show ipv6 eigrp neighbors

IPv6-EIGRP Neighbors for process 77 vrf default

Address                Interface    Holdtime  Uptime    Q      Seq  SRTT  RTO
                   (secs)    (h:m:s)  Count    Num   (ms)  (ms)
2001:0DB8::28          e1/3        13        0:00:41   0      11    4     20
2001:0DB8:2            e4/4        14        0:02:01   0      10   12    24

switch#
```

Table 1-6 describes the significant fields shown in the display.

Table 1-36 *show ip eigrp neighbors Field Descriptions*

Field	Description
process	Autonomous system number specified in the router configuration command.
vrf	VRF name.
Address	IPv6 address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Holdtime	Length of time (in seconds) that the Cisco NX-OS software waits to hear from the peer before declaring that the peer is down.
Uptime	Elapsed time (in hours, minutes, and seconds) since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the software waits to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
SRTT	Smoothed round-trip time. This field indicates the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This field indicates the amount of time that the software waits before resending a packet from the retransmission queue to a neighbor.

The following example shows how to display detailed information about EIGRP neighbors:

```
switch# show ipv6 eigrp neighbors detail

IPv6-EIGRP neighbors for AS 1 vrf default

H   Address                Interface    Hold Uptime    SRTT  RTO  Q  Seq
                   (sec)    (ms)    Cnt  Num
0   2001:0DB9::10          e1/5        14 01:00:52    3   200  0  10

Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 3
```

Send document comments to nexus7k-docfeedback@cisco.com

switch#

Table 1-7 describes the significant fields shown in the display.

Table 1-37 *show ip eigrp neighbors detail Field Descriptions*

Field	Description
Version	Version of EIGRP software running on the node and neighbor.
Retrans:	Number of retransmissions sent to this neighbor.
Retries:	Number of retransmissions sent to this neighbor since the last acknowledgement (ACK).
Prefixes	Number of prefixes learned from this neighbor.

Related Commands

Command	Description
clear ipv6 eigrp neighbors	Clears neighbors for EIGRP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 eigrp route-map statistics

To display the route redistribution statistics for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp route-map statistics** command in any mode.

```
show ipv6 eigrp [instance-tag] route-map statistics redistribute {bgp id | direct | eigrp id | isis
id | ospfv3 id | rip id | static} [vrf {vrf-name | *}]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
vrf *	(Optional) Specifies all VRF instances.
bgp	Displays the policy statistics for the Border Gateway Protocol (BGP).
direct	Displays the policy statistics for directly connected routes only.
eigrp	Displays the policy statistics for EIGRP.
isis	Displays the policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
ospfv3	Displays the policy statistics for the Open Shortest Path First (OSPF) version 3 protocol.
rip	Displays the policy statistics for the Routing Information Protocol (RIP).
static	Displays the policy statistics for IP static routes.
<i>id</i>	For the bgp keyword, the <i>id</i> 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. For the eigrp keyword, the <i>id</i> 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 NX-OS stores it internally as a string. For the isis keyword, the <i>id</i> is an IS-IS 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 NX-OS stores it internally as a string. For the ospf keyword, the <i>id</i> is 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults None

Command Modes Any

■ **show ipv6 eigrp route-map statistics**

Send document comments to nexus7k-docfeedback@cisco.com

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples The following example shows how to display route-map statistics for EIGRP:

```
switch(config)# show ipv6 eigrp route-map statistics redistribute direct
C: No. of comparisons, M: No. of matches
```

```
route-map rmap1 permit 1
```

```
Total accept count for policy: 10
Total reject count for policy: 0
```

Related Commands

Related Commands	Command	Description
	clear ipv6 eigrp route-map statistics	Clears route-map statistics for EIGRP.
	show ipv6 eigrp traffic	Displays EIGRP traffic statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 eigrp topology

To display the Enhanced Interior Gateway Routing Protocol (EIGRP) for an IPv6 topology table, use the **show ipv6 eigrp topology** command.

```
show ipv6 eigrp [instance-tag] topology [ipv6-address/length] [active | all-links | detail-links |  
pending | summary | zero-successors] [vrf {vrf-name | *}]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
<i>ipv6-address/length</i>	(Optional) IP address in A:B::C:D format with a network mask indicated as a slash (/) and number. The length range is from 1 to 128.
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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
vrf *	(Optional) Specifies all VRF instances.

Defaults	This command displays information for the default VRF if no VRF is specified.

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	Use the show ipv6 eigrp topology command to determine Diffusing Update Algorithm (DUAL) states and to debug possible DUAL problems.

Send document comments to nexus7k-docfeedback@cisco.com

When you use the **show ipv6 eigrp topology** command without any keywords or arguments, Cisco NX-OS displays only routes that are feasible successors.

This command requires the Enterprise 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 ipv6 eigrp topology 2001:0DB8::/24

IP-EIGRP (AS 1): Topology entry for 2001:0DB8::/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
Routing Descriptor Blocks:
  2001:0DB8::10 (Ethernet 2/1), from 2001:0DB8::1, Send flag is 0x0
    Composite metric is (409600/128256), Route is External
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 192.0.2.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
switch#
```

Table 1-8 describes the significant fields shown in the display.

Table 1-38 *show ip eigrp topology Field Descriptions*

Field	Description
Query origin	Query origin state.
Successors	Number of feasible successors for this prefix.
FD	Feasible distance for this prefix.
2001:0DB8::10 (Ethernet 2/1)	Next hop and interface from which this path was learned.
from 2001:0DB8::1	Information source for this path.
Send flag	Status of whether the sending of this prefix is pending to this neighbor.
Composite metric is...	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.
Route is	Type of route (internal or external).
Vector Metric	Metric (bandwidth, delay, reliability, load, MTU, and hop count) advertised by the neighbor.
External Data	External information (originating router ID, AS number, external protocol, metric, and tag) advertised by the neighbor.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets sent and received, use the **show ipv6 eigrp traffic** command.

show ipv6 eigrp [*instance-tag*] **traffic** [**vrf** {*vrf-name* | *}]

Syntax Description	<i>instance-tag</i>	(Optional) Name of the EIGRP instance. The instance tag can be any case-sensitive alphanumeric string up to 63 characters.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
	vrf *	(Optional) Specifies all VRF instances.

Defaults	This command displays information for the default VRF if no VRF is specified.

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	Use the show ipv6 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 Enterprise Services license.

Examples	The following example shows how to display the EIGRP traffic statistics:

```
switch# show ipv6 eigrp traffic
```

```
IPv6-EIGRP Traffic Statistics for AS 1 vrf default
```

```
Hellos sent/received: 736/797
Updates sent/received: 6/6
Queries sent/received: 0/1
Replies sent/received: 1/0
Acks sent/received: 6/6
```

Send document comments to nexus7k-docfeedback@cisco.com

```
Input queue high water mark 0, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
```

Table 1-9 describes the significant fields shown in the display.

Table 1-39 *show ipv6 eigrp traffic Field Descriptions*

Field	Description
AS	Autonomous system number specified in the router eigrp command.
vrf	VRF specified in the show command.
Hellos sent/received:	Number of hello packets sent and received.
Updates sent/received:	Number of update packets sent and received.
Queries sent/received:	Number of query packets sent and received.
Replies sent/received:	Number of reply packets sent and received.
Acks sent/received:	Number of acknowledgment packets sent and received.
Input queue high water mark	Maximum number of packets in the input queue and number of drops.
SIA-Queries sent/received	Number of Stuck-in-Active query packets sent and received.
SIA-Replies sent/received:	Number of Stuck-in-Active reply packets sent and received.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 fragments

To display information about the IPv6 fragments queued, use the **show ipv6 fragments** command.

show ipv6 fragments [*ipv6-addr*]

Syntax Description	<i>name</i> (Optional)IPv6 address. The format is A:B::C:D.	
Defaults	None	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the IPv6 fragments: switch(config-if)# show ipv6 fragments No IPv6 fragments queued	
Related Commands	Command	Description
	show ipv6 process	Displays information about the IPv6 process.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 icmp interface

To display information about the ICMPv6, use the **show ipv6 icmp interface** command.

show ipv6 icmp interface [*type number*] [**detail**] [**vrf** *vrf-name*]

Syntax Description	<i>type</i>	(Optional) Interface type. Use ? to see the list of supported interfaces.
	<i>number</i>	(Optional) Interface number. Use ? to see the range.
	detail	(Optional) Displays detailed ICMPv6 information.
	vrf <i>vrf-name</i>	(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

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays ICMPv6 information: switch(config-if)# show ipv6 icmp interface

Related Commands	Command	Description
	ipv6 icmp	Configures ICMPv6 on an interface.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 interface

To display IPv6 information for an interface, use the **show ipv6 interface** command.

show ipv6 interface [*type number*] [**brief**][**vrf** *vrf-name*]

Syntax Description	<i>type</i>	(Optional) Interface type. Use ? to see the options.
	<i>number</i>	(Optional) Interface number. Use ? to see the range.
	brief	(Optional) Displays a summary of IP information.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Command Modes Any

SupportedUserRoles Network Administrator
VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example displays IPv6 information for Ethernet 2/1:

```
switch# show ipv6 interface ethernet 2/1
Ethernet2/1, Interface status: protocol-down/link-down/admin-down, iod: 80
Context:"default"
IPv6 address: 2001:0db8:0000:0000:0000:0000:0000:0001
IPv6 subnet: 2001:0000:0000:0000:0000:0000:0000:0000/16
IPv6 link-local address: fe80::0218:baff:fed8:3ffd (default)
IPv6 multicast routing: disabled
IPv6 multicast groups locally joined:
    ff02::0001:ff00:0001 ff02::0002 ff02::0001 ff02::0001:ffd8:3ffd
IPv6 multicast (S,G) entries joined: none
IPv6 MTU: 1500 (using link MTU)
IPv6 RP inbound packet-filtering policy: none
IPv6 RP outbound packet-filtering policy: none
IPv6 inbound packet-filtering policy: none
IPv6 outbound packet-filtering policy: none
IPv6 interface statistics last reset: never
IPv6 interface RP-traffic statistics: (forwarded/originated/consumed)
    Unicast packets:      0/0/0
    Unicast bytes:        0/0/0
    Multicast packets:    0/0/0
```

 `show ipv6 interface`

Send document comments to nexus7k-docfeedback@cisco.com

```
Multicast bytes:      0/0/0
IPv6 interface hardware statistics not available
Reason: unsupported platform
```

Related Commands

Command	Description
<code>show ip interface</code>	Displays IP information about an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 mbgp

To display entries in the Multiprotocol Border Gateway Protocol (MP-BGP) table, use the **show ipv6 mbgp** command.

```
show ipv6 mbgp [ipv6-addr | ipv6-prefix [longer-prefixes]] [vrf vrf-name]
```

Syntax Description	<i>ipv6-addr</i>	(Optional) A network from the MBGP route table. The format is A:B::C:D.
	<i>ipv6-prefix</i>	(Optional) A prefix from the the MBGP route table. The format is A:B::C:D/length.
	longer-prefixes	(Optional) Displays the prefix and any more specific routes.
	<i>vrf vrf-name</i>	(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	
Supported User Roles	network-admin network-operator vdc-admin vdc-operator	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example displays the MBGP route table: switch(config-router)# show ipv6 mbgp BGP routing table information for VRF default, address family IPv6 Multicast	
Related Commands	Command	Description
	clear ip mbgp	Clears entries in the MBGP route table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 mbgp community

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match a community, use the **show ipv6 mbgp community** command.

```
show ipv6 mbgp community [as-number] [no-advertise] [no-export] [no-export-subconfed]
[exact-match]] [vrf vrf-name]
```

Syntax Description

<i>as-number</i>	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 <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays routes that match a community:

```
switch(config)# show ipv6 mbgp community
```

Related Commands

Command	Description
ipv6 community-list	Creates a community list.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 mbgp community-list

To display Multiprotocol Border Gateway Protocol (MP-BGP) routes that match a community list, use the **show ipv6 mbgp community-list** command.

show ipv6 mbgp community-list *commlist-name* [**exact-match**] [**vrf** *vrf-name*]

Syntax Description	community-list <i>commlist-name</i>	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 <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays routes that match a community list: switch(config)# show ip v6mbgp community-list test1

Related Commands	Command	Description
	ipv6 community-list	Creates a community list.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 mbgp neighbors

To display Multiprotocol Border Gateway Protocol (MP-BGP) neighbors, use the **show ipv6 mbgp neighbors** command.

show ipv6 mbgp neighbors [*addr* [**advertised-routes** | **flap-statistics** | **paths** | **received-routes** | **routes** [**advertised** | **dampened** | **received**]]] [*prefix*] [**vrf** { **all** | *vrf-name* }]

Syntax Description

<i>addr</i>	IPv6 address. The format is A:B::C:D.
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.
<i>prefix</i>	(Optional) IPv6 prefix. The format is A:B::C:D/length.
vrf <i>vrf-name</i>	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
all	(Optional) Specifies all VRFS.

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Added paths keyword.

Usage Guidelines

This command does not require a license.

Examples

This example displays the MBGP neighbors:

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# show ipv6 mbgp neighbors
```

Related Commands	Command	Description
	show ip mbgp neighbors	Displays BGP information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 nd interface

To display information about the Neighbor Discovery (ND), use the **show ipv6 nd interface** command.

show ipv6 nd interface [*type number*] [**detail**] [**vrf** *vrf-name*]

Syntax Description	<i>type</i>	(Optional) Interface type. Use ? to see the list of supported interfaces.
	<i>number</i>	(Optional) Interface number. Use ? to see the range.
	detail	(Optional) Displays detailed ND information.
	vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays ND information: <pre>switch(config-if)# show ipv6 nd interface ICMPv6 ND Interfaces for VRF "default" Ethernet2/45, Interface status: protocol-down/link-down/admin-down IPv6 address: 2001:0db8:0000:0000:0000:0000:0000:0001 ICMPv6 active timers: Last Neighbor-Solicitation sent: never Last Neighbor-Advertisement sent: never Last Router-Advertisement sent: never Next Router-Advertisement sent in: 0.000000 Router-Advertisement parameters: Periodic interval: 200 to 600 seconds Send "Managed Address Configuration" flag: false Send "Other Stateful Configuration" flag: false Send "Current Hop Limit" field: 64 Send "MTU" option value: 1500 Send "Router Lifetime" field: 1800 secs</pre>

Send document comments to nexus7k-docfeedback@cisco.com

```
Send "Reachable Time" field: 0 ms
Send "Retrans Timer" field: 0 ms
Neighbor-Solicitation parameters:
  NS retransmit interval: 1000 ms
ICMPv6 error message parameters:
  Send redirects: true
  Send unreachable: false
```

Related Commands

Command	Description
ipv6 nd	Configures ICMPv6 ND on an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 neighbor

To display IPv6 neighbors, use the **show ipv6 neighbor** command.

show ipv6 neighbor [*ipv6-addr* | *interface*] [**detail**] [**non-best**] [**statistics**] [**summary**] [**vrf** *vrf-name*]

Syntax Description

<i>ipv6-addr</i>	(Optional) An IPv6 source address. The format is A:B::C:D
<i>interface</i>	(Optional) An interface. Use ? to determine the supported interface types.
detail	(Optional) Displays detailed neighbor information.
non-best	(Optional) Displays the best neighbor entries and the alternate neighbor entries.
statistics	(Optional) Displays neighbor statistics.
summary	(Optional) Displays a summary of the neighbor information.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Added non-best and summary keywords.
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show ipv6 neighbor** command to display the IPv6 adjacency table.
This command does not require a license.

Examples

This example displays IPv6 neighbors:

```
switch# show ipv6 neighbor
```

```
IPv6 Adjacency Table for VRF default
Total number of entries: 0
Address          Age          MAC Address      Pref Source      Interface
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	ipv6 nd	Configures ICMPv6 ND on an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 policy

To display the route policy information, use the **show ipv6 policy** command.

show ipv6 policy [**vrf** *vrf-name*]

Syntax Description	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows the policies attached to interfaces:

```
switch(config-if)# show ipv6 policy
Interface      Route-map      Status      VRF-Name
Ethernet2/45   floor1        Inactive    --
```

Related Commands	Command	Description
	ipv6 policy	Configures a route policy on an interface.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 prefix-list

To display prefix lists for the Border Gateway Protocol (BGP), use the **show ipv6 prefix-list** command.

show ipv6 prefix-list [*name*]

Syntax Description	<i>name</i> (Optional) Name of community list. The name can be any case-sensitive alphanumeric string up to 63 characters.				
Defaults	None				
Command Modes	Any command mode				
Supported User Roles	network-admin network-operator vdc-admin vdc-operator				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
Usage Guidelines	This command does not require a license.				
Examples	This example displays the prefix lists: <pre>switch(config)# show ipv6 prefix-list ip prefix-list test2: 1 entries seq 5 permit 2001:0DB8::/8</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ipv6 prefix-list</td><td>Configures a BGP prefix list.</td></tr></table>	Command	Description	ipv6 prefix-list	Configures a BGP prefix list.
Command	Description				
ipv6 prefix-list	Configures a BGP prefix list.				

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 process

To display formation about the IPv6 process, use the **show ipv6 process** command.

show ipv6 process [*vrf vrf-name*]

Syntax Description	<i>vrf vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows details on the IPv6 process: <pre>switch(config)# show ipv6 process VRF default VRF id is 1 Auto discard is disabled Auto discard is not added Static discard is not configured Number of static default route configured is 0 Number of ipv6 unreachable configured is 0 Iodlist: 80 Local address list: 2001:0db8::0001 fe80::0218:baff:fed8:3ffd</pre>

Related Commands	Command	Description
	show ip process	Displays information about the IPv4 process.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 route

To display routes from the unicast RIB, use the **show ipv6 route** command.

show ipv6 route [*addr* | *hostname* | *prefix*] [*route-type*][**summary**] [**vrf** *vrf-name*]

Syntax Description	
<i>addr</i>	(Optional) IPv6 address. The format is A:B::C:D.
<i>hostname</i>	Host name. The <i>name</i> can be any case-sensitive alphanumeric string up to 80 characters.
<i>prefix</i>	(Optional) IPv6 prefix. The format is A:B::C:D/length. The length range is from 1 to 128.
<i>route-type</i>	(Optional) Type of route. Use ? to see the list of types.
summary	(Optional) Displays route counts.
vrf <i>vrf-name</i>	(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

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(3)	This command was introduced.
	4.1(2)	Added <i>hostname</i> argument.

Usage Guidelines	This command does not require a license.

Examples	This example displays the route table:

```
switch(config)# show ipv6 route
IPv6 Routing Table for VRF "default"

0::/127, ubest/mbest: 1/0
    *via 0::, Null0, [220/0], 18:03:20, discard, discard
fe80::/10, ubest/mbest: 1/0
    *via 0::, Null0, [220/0], 18:03:20, discard, discard
```

 show ipv6 route

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
clear ipv6 route	Clears entries in the route table.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 routers

To display IPv6 neighbor routers, use the **show ipv6 routers** command.

show ipv6 routers

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example shows how to display the IPv6 neighbors: switch(config)# show ipv6 routers

Related Commands	Command	Description
	clear ipv6 neighbors	Displays IPv6 neighbor details.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ipv6 static-route

To display static routes from the unicast RIB, use the **show ipv6 static-route** command.

show ipv6 static-route [**vrf** {*vrf-name* | **all**}]

Syntax Description	vrf <i>vrf-name</i>	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive alphanumeric string up to 63 characters.
	all	(Optional) Specifies all virtual router contexts (VRF) name.

Defaults	None

Command Modes	Any command mode

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.2(1)	Added all keyword.

Usage Guidelines	This command does not require a license.

Examples	This example displays the static routes: switch(config)# show ipv6 static-route IPv6 Unicast Static Routes:

Related Commands	Command	Description
	ipv6 route	Configures a static route.

Send document comments to nexus7k-docfeedback@cisco.com

show ipv6 traffic

To display IPv6 traffic information, use the **show ipv6 traffic** command.

show ipv6 traffic

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example displays the IPv6 traffic information: <pre>switch(config)# show ipv6 traffic IPv6 Software Processed Traffic and Error Statistics, last reset: never RP-Traffic Statistics: Counter Unicast Multicast ----- Packets forwarded: 0 0 Bytes forwarded: 0 0 Packets originated: 0 0 Bytes originated: 0 0 Packets consumed: 0 0 Bytes consumed: 0 0 Fragments originated: 0 0 Fragments consumed: 0 0 Error Statistics: Bad version: 0, route lookup failed: 0, hop limit exceeded: 0 Option header errors: 0, payload length too small: 0 PM errors: 0, MBUF errors: 0, encapsulation errors: 0</pre>

 show ipv6 traffic

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
show ipv6 process	Displays information about the IPv6 process.

Send document comments to nexus7k-docfeedback@cisco.com

show isis adjacency

To display adjacency information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis adjacency** command.

show isis [*instance-tag*] **adjacency** [*interface*] [**detail**] [**summary**] [**system-id** *sid*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>interface</i>	(Optional) Interface name. Use ? to determine the supported interface types.
detail	(Optional) Displays detailed adjacency information.
summary	(Optional) Displays a summary of the adjacency information.
system-id <i>sid</i>	(Optional) Displays the adjacency information for this system ID. The <i>sid</i> format is XXXX.XXXX.XXXX.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the adjacency information:

```
switch# show isis adjacency
```

```
IS-IS process: 1 VRF: default
```

```
IS-IS adjacency database:
```

System ID	SNPA	Level	State	Hold Time	Interface
test11-m9	001b.210d.e3bd	1	UP	00:00:07	Ethernet2/3
test11-m9	001b.210d.e3bd	2	UP	00:00:06	Ethernet2/3
test11-m9	0015.1757.d82c	1	UP	00:00:33	Ethernet2/4
test11-m9	0015.1757.d82c	2	UP	00:00:28	Ethernet2/4

Send document comments to nexus7k-docfeedback@cisco.com

```
test11-m9      N/A          1-2    UP      00:00:28  Ethernet2/5
test11-m9      0015.1757.d82f  1      UP      00:00:31  Ethernet2/7
test11-m9      0015.1757.d82f  2      UP      00:00:24  Ethernet2/7
```

The following example shows how to display the adjacency information for Ethernet 2/3 and system ID test11-m9:

```
switch# show isis adjacency ethernet 2/3 system-id test1
IS-IS process: 1 VRF: default
IS-IS adjacency database for Ethernet2/3:
System ID      SNPA          Level  State  Hold Time  Interface
test11-m9      001b.210d.e3bd  1      UP      00:00:08  Ethernet2/3
  Up/Down transitions: 1, Last transition: 00:06:44 ago
  Circuit Type: L1-2
  IPv4 Address: 23.1.1.9
  IPv6 Address: 0::
  Circuit ID: test11-m9.01, Priority: 64

test11-m9      001b.210d.e3bd  2      UP      00:00:06  Ethernet2/3
  Up/Down transitions: 1, Last transition: 00:06:37 ago
  Circuit Type: L1-2
  IPv4 Address: 23.1.1.9
  IPv6 Address: 0::
  Circuit ID: test11-m9.01, Priority: 64
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

show isis database

To display database information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis database** command.

```
show isis [instance-tag] database [lspid] [detail | summary] [level-1 | level-2] [{adjacency sid] |  
[{ip | ipv6} prefix filter] | [router-id id] | [zero-sequence] [vrf vrf-name]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>lspid</i>	(Optional) LSP ID. The <i>sid</i> format is XXXX.XXXX.XXXX.XX-XX.
detail	(Optional) Displays detailed database information.
summary	(Optional) Displays a summary of the database information.
level-1	(Optional) Displays Level 1 router database information.
level-2	(Optional) Displays Level 2 router database information.
adjacency <i>sid</i>	(Optional) Displays database information that matches the adjacency filter. The <i>sid</i> format is XXXX.XXXX.XXXX.XX.
{ ip ipv6 } prefix <i>filter</i>	(Optional) Displays database information that matches the prefix filter. The <i>filter</i> format for IPv4 is x.x.x.x/length, where the length range is from 1 to 32. The <i>filter</i> format for IPv6 is A:B::C:D/length, where the length range is from 1 to 128.
router-id <i>id</i>	(Optional) Displays database information that matches the router ID. The <i>id</i> format is x.x.x.x.
zero-sequence	(Optional) Displays the database information for LSPs with zero sequence numbers.
vrf <i>vrf-name</i>	(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

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example shows how to display the database information:

```
switch# show isis database

IIS-IS Process: 1 LSP database VRF: default
IS-IS Level-1 Link State Database
  LSPID           Seq Number   Checksum   Lifetime   A/P/O/T
  test11-m9.00-00  0x000006AB  0xD715    1115      0/0/0/3
  test11-m9.01-00  0x00000002  0xB7DF    1008      0/0/0/3
  test-m10.00-00   * 0x0000000C  0xC457    1125      0/0/0/3
  test-m10.02-00   * 0x00000002  0x8673    1024      0/0/0/3
  test-m10.04-00   * 0x00000002  0x787F    1029      0/0/0/3

IS-IS Level-2 Link State Database
  LSPID           Seq Number   Checksum   Lifetime   A/P/O/T
  test11-m9.00-00  0x0000065F  0x98A0    1115      0/0/0/3
  test11-m9.01-00  0x00000002  0xB7DF    1067      0/0/0/3
  test-m10.00-00   * 0x0000000C  0x1903    1125      0/0/0/3
  test-m10.02-00   * 0x00000002  0x8673    1018      0/0/0/3
  test-m10.04-00   * 0x00000002  0x787F    1040      0/0/0/3
```

The following example shows how to display the detailed database information for test11-m9:

```
switch(config)# show isis database level-1 detail test11-m9.00-00
IS-IS Process: 1 LSP database VRF: default
IS-IS Level-1 Link State Database
  LSPID           Seq Number   Checksum   Lifetime   A/P/O/T
  test11-m9.00-00  0x000006AB  0xD715    1079      0/0/0/3
  Instance       : 0x00000006
  Area Address   : 48
  NLPID          : 0xCC 0x8E
  Router ID      : 9.1.1.1
  IP Address     : 9.1.1.1
  Hostname       : test11-m9      Length : 9
  Extended IS    : test-m10.02    Metric : 40
  Extended IS    : test-m10.04    Metric : 40
  Extended IS    : test11-m9.01    Metric : 400
  Extended IS    : test-m10.00    Metric : 40
  Extended IP    : 25.1.1.0/24    Metric : 40      (U)
  Extended IP    : 24.1.1.0/24    Metric : 40      (U)
  Extended IP    : 80.1.1.0/24    Metric : 10      (U)
  Extended IP    : 70.1.1.0/24    Metric : 10      (U)
  Extended IP    : 60.1.1.0/24    Metric : 10      (U)
  Extended IP    : 50.1.1.0/24    Metric : 10      (U)
  Extended IP    : 23.1.1.0/24    Metric : 400     (U)
  Extended IP    : 9.1.1.0/24     Metric : 1       (U)
  IPv6 Prefix    : 0027::/64     Metric : 40      (U/I)
  Digest Offset  : 0
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

show isis hostname

To display hostname information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis hostname** command.

show isis [*instance-tag*] **hostname** [**detail**] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
detail	(Optional) Displays detailed hostname information.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the hostname information:

```
test11-m9# show isis hostname
IS-IS Process: 1 dynamic hostname table VRF: default
  Level  System ID      Dynamic hostname
  ---  -
  1      0015.1757.d82c    test11-m9
  1      0015.1757.d8c8*  test-m10
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis interface

To display interface information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis interface** command.

show isis [*instance-tag*] **interface** [*interface*] [**brief**] [**level-1** | **level-2**] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>interface</i>	(Optional) Interface name and interface number. Use ? to see a list of interfaces.
brief	(Optional) Displays a summary of the interface information.
level-1	(Optional) Displays Level 1 interface information.
level-2	(Optional) Displays Level 2 interface information.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display a brief view of the interface information:

```
switch# show isis interface brief
```

```
IIS-IS process: 1 VRF: default
Interface      Type  Idx  State      Circuit  MTU  Metric  Priority  Adjs/AdjsUp
              L1   L2   L1   L2   L1   L2   L1   L2   L1   L2
loopback1      Loop  5    Up/Ready    0x01/L1-2 1500 1   1   64   64   0/0   0/0
Ethernet2/3     Bcast 1    Up/Ready    0x01/L1-2 1500 400 400 64   64   1/1   1/1
Ethernet2/4     Bcast 2    Up/Ready    0x02/L1-2 1500 40   40   64   64   1/1   1/1
Ethernet2/5     P2P   3    Up/Ready    0x01/L1-2 1500 40   40   64   64   1/1   1/1
Ethernet2/6     Bcast 4    Down/Ready  0x03/L1-2 1500 40   40   64   64   0/0   0/0
```

Send document comments to nexus7k-docfeedback@cisco.com

```
Ethernet2/7 Bcast 6 Up/Ready 0x04/L1-2 1500 40 40 64 64 1/1 1/1
```

The following example shows how to display the interface information for Ethernet 2/5:

```
switch# show isis interface ethernet 2/5
IS-IS process: 1 VRF: default
Ethernet2/5, Interface status: protocol-up/link-up/admin-up
  IP address: 192.0.2.1 IP subnet: 192.0.2.0/24
  IPv6 routing is disabled
  Index: 0x0003, Local Circuit ID: 0x01, Circuit Type: L1-2
  Extended Local Circuit ID: 0x1A084000, P2P Circuit ID: 0000.0000.0000.00
  Retx interval: 5, Retx throttle interval: 66 ms
  LSP interval: 33 ms, MTU: 1500
  P2P Adjs: 1, AdjsUp: 1, Priority 64
  Hello Interval: 10, Multi: 3, Next IIH: 00:00:08
Level   Adjs   AdjsUp  Metric   CSNP   Next CSNP   Last LSP ID
1       1       1       40       60     00:00:48   ffff.ffff.ffff.ff-ff
2       1       1       40       60     00:00:19   ffff.ffff.ffff.ff-ff
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis ip route-map statistics redistribute

To display statistics for route redistribution for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis ip route-map statistics redistribute** command.

```
show isis [instance-tag] ip route-map statistics redistribute { bgp id | direct | eigrp id | isis id |
ospf id | rip id | static } [vrf vrf-name]
```

Syntax Description		
<i>instance-tag</i>		(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
bgp		Displays statistics for the Border Gateway Protocol (BGP).
direct		Displays statistics for directly connected routes only.
eigrp		Displays statistics for the Enhanced Interior Gateway Protocol (EIGRP) routing protocol.
isis		Displays statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
ospf		Displays statistics for the Open Shortest Path First (OSPF) protocol.
rip		Displays statistics for the Routing Information Protocol (RIP).
static		Displays statistics for IP static routes.
<i>id</i>		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 isis , eigrp , 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i>		(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

Use the **show isis ip route-map statistics redistribute** command to display redistribution statistics. This command requires the Enterprise Services license.

Examples

This example shows how to display statistics for redistributed routes:

```
switch# show isis ip route-map statistics redistribute static
IS-IS process: 1
VRF: default
C: No. of comparisons, M: No. of matches

route-map rm10 permit 10

Total accept count for policy: 9
Total reject count for policy: 0
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis mesh-group

To display mesh groups for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis mesh-group** command.

show isis [*instance-tag*] **mesh-group** [*number*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>number</i>	(Optional) Number of the IS-IS mesh group. The range is from 1 to 4294967295.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the mesh groups:

```
switch# show isis mesh-group
IS-IS Process: Test1 mesh-groups VRF: default
Mesh-group 33:
  Ethernet7/45
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

Send document comments to nexus7k-docfeedback@cisco.com

show isis protocol

To display process-level information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis protocol** command.

show isis [*instance-tag*] [**protocol**] [**vrf** *vrf-name*]

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
vrf <i>vrf-name</i>	(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

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to display the IS-IS protocol information:

```
switch# show isis protocol
ISIS process : 1
VRF: default
  System ID : 0015.1757.d8c8  IS-Type : L1-L2
  SAP : 412  Queue Handle : 11
  Graceful Restart enabled
  Metric-style : advertise(wide), accept(narrow, wide)
  Area address(es) :
    48
  Process is up and running
  VRF ID: 1
  Stale routes during non-graceful controlled restart
  Interfaces supported by IS-IS :
    loopback1
    Ethernet2/3
    Ethernet2/4
```

Send document comments to nexus7k-docfeedback@cisco.com

```
Ethernet2/5
Ethernet2/6
Ethernet2/7
Address family IPv4 unicast :
  Number of interface : 5
  Distance : 115
Address family IPv6 unicast :
  Number of interface : 1
  Distance : 115
L1 Next SPF: Inactive
L2 Next SPF: Inactive
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis redistribute route

To display route redistribution information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis redistribute route** command.

```
show isis [instance-tag] [ip | ipv6] redistribute route [address | prefix] [longer-prefixes
[summary]] | summary [vrf vrf-name]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
ip	(Optional) Displays route redistribution information for an IPv4 route.
ipv6	(Optional) Displays route redistribution information for an IPv6 route.
<i>address</i>	(Optional) Route redistribution information for a specific IPv4 or IPv6 address. The <i>address</i> format for IPv4 is x.x.x.x. The <i>address</i> format for IPv6 is A:B::C:D.
<i>prefix</i>	(Optional) Route redistribution information for a specific IPv4 or IPv6 address. The <i>prefix</i> format for IPv4 is x.x.x.x/length, where the length range is from 1 to 32. The <i>prefix</i> format for IPv6 is A:B::C:D/length, where the length range is from 1 to 128.
longer-prefixes	(Optional) Displays the exact match to the prefix as well as more specific routes.
summary	(Optional) Displays a summary of the route redistribution information.
vrf <i>vrf-name</i>	(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

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to display the route redistribution information:

```
switch# show isis redistribute route
```

```
IS-IS process: 1 VRF: default
```

Send document comments to nexus7k-docfeedback@cisco.com

```
IS-IS IPv4 redistribute route

100.1.1.1/32, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.1.1.2/32, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.1.1.3/32, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.1.1.4/32, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.2.0.0/16, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.2.1.0/24, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.2.1.1/32, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
```

The following example shows how to display the route redistribution information for route 100.2.1.0:

```
test-m10(config)# show isis redistribute route 100.2.1.0/16 longer-prefixes
IS-IS process: 1 VRF: default
IS-IS IPv4 redistribute route

100.2.0.0/16, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.2.1.0/24, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
100.2.1.1/32, static,
  Redistributed into L1, metric 10
  Redistributed into L2, metric 10
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis route

To display route information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis route** command.

```
show isis [instance-tag] [ip | ipv6] route [address | prefix [longer-prefixes [summary]] [detail |  
summary] [vrf vrf-name]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
ip	(Optional) Displays route information for an IPv4 route.
ipv6	(Optional) Displays route information for an IPv6 route.
<i>address</i>	(Optional) Route information for a specific IPv4 or IPv6 address. The <i>address</i> format for IPv4 is x.x.x.x. The <i>address</i> format for IPv6 is A:B::C:D.
<i>prefix</i>	(Optional) Route information for a specific IPv4 or IPv6 address. The <i>prefix</i> format for IPv4 is x.x.x.x/length, where the length range is from 1 to 32. The <i>prefix</i> format for IPv6 is A:B::C:D/length, where the length range is from 1 to 128.
longer-prefixes	(Optional) Displays the exact match to the prefix as well as more specific routes.
summary	(Optional) Displays a summary of the route information.
detail	(Optional) Displays detailed route information.
vrf <i>vrf-name</i>	(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

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	The following example shows how to display the route information for IPv4:

```
switch# show isis route
```

Send document comments to nexus7k-docfeedback@cisco.com

```
IS-IS IPv4 routing table

10.1.1.0/24, L1, direct
    *via GigabitEthernet2/1, metric 40, L1, direct
    via GigabitEthernet2/1, metric 40, L2, direct
10.1.2.0/24, L1, direct
    *via GigabitEthernet2/2, metric 40, L1, direct
    via GigabitEthernet2/2, metric 40, L2, direct
100.0.0.2/32, L1, direct
    *via Loopback0, metric 1, L1, direct
    via Loopback0, metric 1, L2, direct
```

The following example shows how to display the route information for IPv6:

```
switch# show isis ipv6 route
IS-IS IPv6 routing table

3000:0010:0001::/48, L1, direct
    *via GigabitEthernet2/1, metric 40, L1, direct
    via GigabitEthernet2/1, metric 40, L2, direct
```

The following example shows how to display the route information for 10.0.0:

```
switch# show isis ip route 10.0.0.0/8 longer-prefixes
IS-IS IPv4 routing table

10.1.1.0/24, L1, direct
    *via GigabitEthernet2/1, metric 40, L1, direct
    via GigabitEthernet2/1, metric 40, L2, direct
10.1.2.0/24, L1, direct
    *via GigabitEthernet2/2, metric 40, L1, direct
    via GigabitEthernet2/2, metric 40, L2, direct
```

The following example shows how to display a summary of the route information for 10.0.0:

```
test-il# show isis ip route 10.0.0.0/8 longer-prefixes summary
IS-IS IPv4 routing table

Summary information for range 10.0.0.0/8

Total number of best routes   : 2
Total number of paths         : 4
Total number of best paths    : 2
Total number of backup paths  : 2

Best routes per level
  L1          total    : 2
              direct   : 2

Best paths per level
  L1          total    : 2
              direct   : 2

Backup paths per level
  L2          total    : 2
              direct   : 2

Number of best routes per mask-length
  /24 : 2
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis route-map statistics distribute

To display statistics for route distribution between Level-1 and Level-2 areas for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis route-map statistics distribute** command.

```
show isis [instance-tag] [ip | ipv6] route-map statistics distribute [level-1 | level-2] into [level-1 | level-2] [vrf vrf-name]
```

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
ip	(Optional) Displays statistics for IPv4.
ipv6	(Optional) Displays statistics for IPv6.
level-1	(Optional) Displays Level 1 distribution statistics.
level-2	(Optional) Displays Level 2 distribution statistics.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display a summary of the distribute information:

```
switch# show isis route-map statistics distribute level-1 into level 2
```

Related Commands

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis rrm

To display Retransmit-Routing-Message (RRM) information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis rrm** command.

show isis [*instance-tag*] **rrm** *interface* [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>interface</i>	Interface name and interface number. Use ? to see a list of interfaces.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the RRM statistics:

```
switch# show isis rrm ethernet 2/3
```

```
IS-IS process: 1
```

```
IS-IS RRM information for interface Ethernet2/3:
  No retransmission on non-P2P interface
```

```
test-m10(config)# show isis rrm eth 2/5
IS-IS process: 1
```

```
IS-IS RRM information for interface Ethernet2/5:
IS-IS Level-1 Link State Database
  Retx interval: 5, Retx throttle interval: 66 ms
  Retx queue length: 0, Next Retx: Inactive
  Retx queue HWM: 5, Retx queue exceed: 0
```

Send document comments to nexus7k-docfeedback@cisco.com

```
LSPID                               Seq Number  Checksum  Lifetime  A/P/O/T  Ago

IS-IS Level-2 Link State Database
Retx interval: 5, Retx throttle interval: 66 ms
Retx queue length: 0, Next Retx: Inactive
Retx queue HWM: 5, Retx queue exceed: 0
LSPID                               Seq Number  Checksum  Lifetime  A/P/O/T  Ago
```

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis spf-log

To display shortest path first (SPF) information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis srm** command.

show isis [*instance-tag*] **spf-log** [**detail**] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
detail	(Optional) Displays detailed information about the SPF calculation.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the SPF information:

```
switch# show isis spf-log
```

```
ITotal number of SPF calculations: 10
```

```
Log entry (current/max): 7/20
```

Ago	Level	Reason	Count	Total
1w0d	1	Adjust route distribution	3	
	2	Adjust route distribution	3	0.000216
1w0d	1	New IP address on GigabitEthernet	1	
	2	New IP address on GigabitEthernet	1	0.000229
1w0d	2	New NH to test-i2 on GigabitEthernet	1	0.000135
1w0d	2	New adj test-i2 on GigabitEthernet	4	0.000243
1w0d	1	New adj test-i2 on GigabitEthernet	3	0.000155
1w0d	1	New LSP test-i2.00-00	2	0.000252
1w0d	1	Updated LSP test-i2.00-00	1	

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis srm

To display Send-Routing-Message (SRM) information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis srm** command.

show isis [*instance-tag*] **srm** *interface* [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>interface</i>	Interface name and interface number. Use ? to see a list of interfaces.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the SRM statistics:

```
switch# show isis srm ethernet 2/3
```

```
IS-IS process: 1
```

```
IS-IS SRM information for interface Ethernet2/3:
```

```
IS-IS Level-1 Link State Database
```

```
Interface is eligible for flooding LSP
```

```
Interface is on stopped SRM list
```

```
LSP interval: 33 ms, Next LSP: Inactive
```

```
LSPID           Seq Number    Checksum    Lifetime    A/P/O/T
```

```
IS-IS Level-2 Link State Database
```

```
Interface is eligible for flooding LSP
```

```
Interface is on stopped SRM list
```

```
LSP interval: 33 ms, Next LSP: Inactive
```


Send document comments to nexus7k-docfeedback@cisco.com

LSPID

Seq Number

Checksum

Lifetime

A/P/O/T

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis ssn

To display Send-Sequence-Number (SSN) information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis ssn** command.

show isis [*instance-tag*] **ssn** *interface* [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>interface</i>	Interface name and interface number. Use ? to see a list of interfaces.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the SSN statistics:

```
switch# show isis ssn ethernet 2/5
```

```
IS-IS SSN information for interface Ethernet2/5:
IS-IS Level-1 Link State Database
  Interface is eligible for sending PSNP
  Next PSNP: Inactive
  LSPID              Seq Number   Checksum  Lifetime   A/P/O/T

IS-IS Level-2 Link State Database
  Interface is eligible for sending PSNP
  Next PSNP: Inactive
  LSPID              Seq Number   Checksum  Lifetime   A/P/O/T
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis statistics

To display statistics for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis statistics** command.

show isis [*instance-tag*] **statistics** [*interface*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>interface</i>	(Optional) Interface name and interface number. Use ? to see a list of interfaces.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the IS-IS statistics:

```
switch# show isis statistics ethernet 7/45
```

```
VRF:                default
SPF calculations:    34
LSPs sourced:        6
LSPs refreshed:     42
LSPs purged:         0
DIS elections:       10
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis summary-address

To display summary address information for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis summary-address** command.

show isis [*instance-tag*] [**ip** | **ipv6**] **summary-address** [*address* | *prefix*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
ip	(Optional) Displays summary address information for IPv4.
ipv6	(Optional) Displays summary address information for IPv6.
<i>address</i>	(Optional) IPv4 or IPv6 address. The <i>address</i> format for IPv4 is x.x.x.x. The <i>address</i> format for IPv6 is A:B::C:D.
<i>prefix</i>	(Optional) IPv4 or IPv6 address. The <i>prefix</i> format for IPv4 is x.x.x.x/length, where the length range is from 1 to 32. The <i>prefix</i> format for IPv6 is A:B::C:D/length, where the length range is from 1 to 128.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display summary address information:

```
switch# show isis summary-address
IS-IS IPv4 summary address:

20.0.0.0/8, L1-2
  Summarize 0 routes into L1
  Summarize 0 routes into L2
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show isis traffic

To display traffic statistics for Intermediate-System-to-Intermediate System (IS-IS), use the **show isis traffic** command.

show isis [*instance-tag*] **traffic** [*interface*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the IS-IS instance. The name can be any case-sensitive alphanumeric string up to 63 characters.
<i>interface</i>	(Optional) Interface name and interface number. Use ? to see a list of interfaces.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

The following example shows how to display the traffic statistics:

```
switch# show isis traffic
IS-IS process: 1
VRF: default
IS-IS Traffic:
%PDU      Received      Sent  RcvAuthErr  OtherRcvErr  ReTransmit
LAN-IIH   62156             87080         0            0            n/a
P2P-IIH   6232              6234         0            0            n/a
CSNP     11646            22356         0            0            n/a
PSNP       802              590          0            0            n/a
LSP      2385             3291         0            0            0
```


Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature isis	Enables IS-IS on the router.
	router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3

To display general information about Open Shortest Path First version 3 (OSPFv3) routing instances, use the **show ospfv3** command.

show [**ipv6**] **ospfv3** [*instance-tag*] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Use this tag to display OSPFv3 information about a specific OSPFv3 instance. The <i>instance-tag</i> argument can be any alphanumeric string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show ospfv3** command to display information about one or more OSPFv3 instances. This command requires the Enterprise Services license.

Examples

This example shows how to display information about one specific OSPFv3 instance:

```
switch# show ospfv3 201
Routing Process sd with ID 0.0.0.0 vrf default
Graceful-restart is configured
  grace period: 60, state: (null)
  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
Minimum hold time for Router LSA throttle 5000.000 ms
Minimum hold time for Network LSA throttle 5000.000 ms
```

Send document comments to nexus7k-docfeedback@cisco.com

```

Minimum hold time for Intra-Area-Prefix LSA throttle 5000.000 ms
Minimum hold time for Link LSA throttle 5000.000 ms
Minimum LSA arrival 1000.000 msec
Maximum paths to destination 8
Number of external LSAs 0, checksum sum 0
Number of areas is 2, 2 normal, 0 stub, 0 nssa
Number of active areas is 0, 0 normal, 0 stub, 0 nssa
  Area BACKBONE(0) (Inactive)
    Area has existed for 01:13:04
    Interfaces in this area: 1 Active interfaces: 0
    SPF calculation has run 1 times
    Last SPF ran for 0.000433s
    Area ranges are
    Number of LSAs: 0, checksum sum 0
  Area (33) (Inactive)
    Area has existed for 01:13:04
    Interfaces in this area: 0 Active interfaces: 0
    SPF calculation has run 1 times
    Last SPF ran for 0.000053s
    Area ranges are
    Number of LSAs: 0, checksum sum 0

```

Table 1-10 describes the significant fields shown in the display.

Table 1-40 ***show ospfv3 Field Descriptions***

Field	Description
Routing Process...	OSPFv3 instance tag and OSPFv3 router ID.
Stateful High Availability	Status of stateful restart capability.
Graceful-restart	Status of graceful restart configuration.
grace period	Number of seconds that OSPFv3 has to trigger a graceful restart.
Last graceful restart exit status	Exit status for last graceful restart.
Supports...	Number of types of service supported (Type 0 only).
Reference Bandwidth	Bandwidth used for cost calculation.
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum LSA arrival	Minimum interval between link-state advertisements.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 border-routers

To display the Open Shortest Path First version 3 (OSPFv3) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ospfv3 border-routers** command.

show [**ipv6**] **ospfv3** [*instance-tag*] **border-routers** [**vrf** *vrf-name*]

Syntax Description		
<i>instance-tag</i>		(Optional) Name of the OSPF instance. Use this tag to display OSPFv3 information about a specific OSPFv3 instance. The <i>instance-tag</i> argument can be any alphanumeric string.
vrf <i>vrf-name</i>		(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the show ospfv3 border-routers command to display information on ABRs. and ASBRs. This command requires the Enterprise Services license.

Examples	This example shows how to display information about border routers:

```
switch# show ospfv3 border-routers

OSPFv3 Process ID p1, vrf default internal routing table
Codes: i - Intra-area route, I - Inter-area route

i 60.60.60.60 [10], ABR, Area 0.0.0.0, SPF 9
   via fe80::0206:d6ff:fec8:a41c, Ethernet2/5
i 60.60.60.60 [10], ABR, Area 0.0.0.1, SPF 9
   via fe80::0206:d6ff:fec8:a408, Ethernet2/6
```

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-11 describes the significant fields shown in the display.

Table 1-41 ***show ospfv3 border-routers Field Descriptions***

Field	Description
40.40.40.40	Router ID of the destination.
[10]	Cost of using this route.
ABR	Router type of the destination; the type is either an ABR, ASBR, or both.
Area	Area ID of the area from which this route is learned.
SPF 71	Internal number of the shortest path first (SPF) calculation that installs this route.
via fe80::0206:d6ff:fec8:a41c	Next hop toward the destination.
Ethernet2/1	Interface type for the outgoing interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 database

To display the Open Shortest Path First version 3 (OSPFv3) database for a specific router, use the **show ospfv3 database** command.

```
show [ipv6] ospfv3 [instance-tag] database [area-id] [link-state-id] [adv-router ip-address |
self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database asbr-summary [area-id] [link-state-id] [adv-router
ip-address | self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database database-summary [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database external [ext_tag value] [link-state-id] [adv-router
ip-address | self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database network [area-id] [link-state-id] [adv-router
ip-address | self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database nssa-external [area-id] [link-state-id] [adv-router
ip-address | self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database opaque-area [area-id] [link-state-id] [adv-router
ip-address | self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database opaque-as [link-state-id] [adv-router ip-address |
self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database opaque-link [area-id] [link-state-id] [adv-router
ip-address | self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database router [area-id] [link-state-id] [adv-router ip-address
| self-originated] [detail] [vrf vrf-name]

show [ipv6] ospfv3 [instance-tag] database summary [area-id] [link-state-id] [adv-router
ip-address | self-originated] [detail] [vrf vrf-name]
```

Syntax Description

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
<i>area-id</i>	(Optional) Area number used to define the particular area. Specify as either an IP address or a number from 0 to 4294967295.
<i>link-state-id</i>	(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.

Send document comments to nexus7k-docfeedback@cisco.com

external	(Optional) Displays information about the external LSAs.
ext_tag <i>value</i>	(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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 ospfv3 database** command to display information about different OSPFv3 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 OSPFv3 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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to display the OSPFv3 database:

```
Router# show ospfv3 database
```

```
OSPFv3 Router with ID (40.40.40.40) (Process ID p1)
```

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Link Count
0.0.0.0	40.40.40.40	301	0x80000006d	1
0.0.0.0	60.60.60.60	1655	0x80000a59	1

Network Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Routers
0.0.0.5	60.60.60.60	1655	0x80000005c	2

Inter-Area Prefix Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Prefix
0.0.0.2	40.40.40.40	301	0x80000006a	1111:2222::/32
0.0.0.4	40.40.40.40	291	0x800000066	1111:6666::/32
0.0.0.6	40.40.40.40	291	0x800000066	6161:6161::6161/128
0.0.0.0	60.60.60.60	147	0x800009f6	6161:6161::6161/128
0.0.0.111	60.60.60.60	1655	0x80000005c	1111:6666::/32
0.0.0.112	60.60.60.60	1655	0x80000005c	1111:2222::/32

Intra-Area Prefix Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Ref-lstype	Ref-LSID
1.0.0.0	40.40.40.40	301	0x80000006e	Router	0.0.0.0
0.0.0.0	60.60.60.60	1655	0x80000a32	Router	0.0.0.0
0.0.3.237	60.60.60.60	1655	0x80000005c	Network	0.0.0.5

Link-Local Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Interface
0.0.0.1	40.40.40.40	341	0x800000066	Enet2/1
0.0.0.3	40.40.40.40	341	0x800000066	Enet24
0.0.0.4	40.40.40.40	301	0x80000006d	Enet25
0.0.0.5	60.60.60.60	147	0x80000917	Enet25

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Link Count
0.0.0.0	40.40.40.40	291	0x80000006d	1
0.0.0.0	60.60.60.60	1655	0x80000abd	1

Network Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Routers
0.0.0.4	60.60.60.60	1655	0x80000005c	2

Inter-Area Prefix Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Prefix
0.0.0.1	40.40.40.40	291	0x80000006a	1111:1111::/32
0.0.0.3	40.40.40.40	331	0x800000066	1111:4444::0001/128
0.0.0.5	40.40.40.40	291	0x800000066	6060:6060::6060/128
0.0.0.0	60.60.60.60	147	0x800009f6	6060:6060::6060/128
0.0.0.156	60.60.60.60	409	0x80000005d	1111:5555::/32
0.0.0.158	60.60.60.60	1655	0x80000005c	1111:1111::/32
0.0.0.159	60.60.60.60	1655	0x80000005c	1111:4444::0001/128

Send document comments to nexus7k-docfeedback@cisco.com

Intra-Area Prefix Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Ref-lstyp	Ref-LSID
1.0.0.0	40.40.40.40	291	0x80000006e	Router	0.0.0.0
0.0.0.0	60.60.60.60	1655	0x800000a54	Router	0.0.0.0
0.0.3.236	60.60.60.60	1655	0x80000005c	Network	0.0.0.4

Link-Local Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Interface
0.0.0.2	40.40.40.40	341	0x800000066	Enet2/2
0.0.0.5	40.40.40.40	291	0x80000006d	Enet2/6
0.0.0.4	60.60.60.60	1655	0x80000005d	Enet2/6

Table 1-12 describes the significant fields shown in the display.

Table 1-42 *show ospfv3 database Field Descriptions*

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router's ID.
Age	Link state age.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	Checksum of the complete contents of the link state advertisement.
Link count	Number of interfaces detected for the router.

This example shows how to display a summary of autonomous system border routers:

```
Router# show ospfv3 database asbr-summary
```

```
OSPFv3 Router with id(192.168.239.66) (Process ID 300)
```

Displaying Summary ASB Link States(Area 0.0.0.0)

```
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0 TOS: 0 Metric: 1
```

Table 1-13 describes the significant fields shown in the display.

Table 1-43 *show ospfv3 database asbr-summary Field Descriptions*

Field	Description
OSPFv3 Router with id	Router ID number.
Process ID	OSPFv3 process ID.
LS age	Link state age.
Options	Type of service options (Type 0 only).

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-43 *show ospfv3 database asbr-summary Field Descriptions (continued)*

Field	Description
LS Type	Link state type.
Link State ID	Link state ID (autonomous system boundary router).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	Checksum of the complete contents of the link state advertisement.
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link state metric.

This example shows how to display information about external links:

```
Router# show ospfv3 database external

OSPFv3 Router with id(192.168.239.66) (Autonomous system 300)

    Displaying AS External Link States

LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.105.0.0 (External Network Number)
Advertising Router: 172.16.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 1
    Forward Address: 0.0.0.0
    External Route Tag: 0
```

Table 1-14 describes the significant fields shown in the display.

Table 1-44 *show ospfv3 database external Field Descriptions*

Field	Description
OSPFv3 Router with id	Router ID number.
Autonomous system	OSPFv3 autonomous system number (OSPFv3 process ID).
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (external network number).
Advertising Router	Advertising router's ID.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-44 *show ospfv3 database external Field Descriptions (continued)*

Field	Description
LS Seq Number	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	Checksum of the complete contents of the LSA.
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
Metric Type	External type.
TOS	Type of service.
Metric	Link state metric.
Forward Address	Forwarding address. Data traffic for the advertised destination will be forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
External Route Tag	External route tag; a 32-bit field attached to each external route. This field is not used by the OSPFv3 protocol itself.

This example shows how to display a summary of the OSPFv3 database:

```
Router# show ospfv3 database database-summary

OSPFv3 Router with ID (100.0.0.1) (Process ID 1)

Area 0 database summary
  LSA Type      Count    Delete    Maxage
  Router        3         0         0
  Network       0         0         0
  Summary Net   0         0         0
  Summary ASBR  0         0         0
  Type-7 Ext    0         0         0
    Self-originated Type-7  0
  Opaque Link   0         0         0
  Opaque Area   0         0         0
  Subtotal      3         0         0

Process 1 database summary
  LSA Type      Count    Delete    Maxage
  Router        3         0         0
  Network       0         0         0
  Summary Net   0         0         0
  Summary ASBR  0         0         0
  Type-7 Ext    0         0         0
  Opaque Link   0         0         0
  Opaque Area   0         0         0
  Type-5 Ext    0         0         0
    Self-originated Type-5  200
  Opaque AS     0         0         0
  Total         203        0         0
```

Table 1-15 describes the significant fields shown in the display.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-45 *show ospfv3 database database-summary Field Descriptions*

Field	Description
Area 0 database summary	Area number.
Count	Count of LSAs of the type identified in the first column.
Router	Number of router link state advertisements in that area.
Network	Number of network link state advertisements in that area.
Summary Net	Number of summary link state advertisements in that area.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that area.
Type-7 Ext	Type-7 LSA count.
Self-originated Type-7	Self-originated Type-7 LSA.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count.
Subtotal	Sum of LSAs for that area.
Delete	Number of link state advertisements that are marked “Deleted” in that area.
Maxage	Number of link state advertisements that are marked “Maxaged” in that area.
Process 1 database summary	Database summary for the process.
Count	Count of LSAs of the type identified in the first column.
Router	Number of router link state advertisements in that process.
Network	Number of network link state advertisements in that process.
Summary Net	Number of summary link state advertisements in that process.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that process.
Type-7 Ext	Type-7 LSA count.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count.
Type-5 Ext	Type-5 LSA count.
Self-Originated Type-5	Self-originated Type-5 LSA count.
Opaque AS	Type-11 LSA count.
Total	Sum of LSAs for that process.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 interface

To display Open Shortest Path First version 3 (OSPFv3)-related interface information, use the **show ospfv3 interface** command.

```
show [ipv6] ospfv3 interface [instance-tag] [interface-type interface-number] [brief] [vrf vrf-name]
```

Syntax Description	<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
	<i>interface-type</i>	(Optional) Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
	<i>interface-number</i>	(Optional) Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.
	brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses, masks, and areas on the router.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.
Defaults	None	
Command Modes	Any	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Use the show ospfv3 interface command to display the OSPFv3 status for the interface. This command requires the Enterprise Services license.	
Examples	This example shows how to display OSPFv3 information for Ethernet interface 1/2: switch# show ospfv3 interface ethernet 1/2 Ethernet1/2 is up, line protocol is up	

Send document comments to nexus7k-docfeedback@cisco.com

```
IP address 192.0.2.1, Process ID 201 vrf default, area 10
IPv6 address 2001:0DB8::1
  Process ID sd vrf default, Instance ID 0, area 0
  State DOWN, Network type P2P, cost 65535
  Index 1, Transmit delay 1 sec
  0 Neighbors, flooding to 0, adjacent with 0
  Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
  Number of link LSAs: 0, checksum sum 0
```

Table 1-16 describes the significant fields shown in the display.

Table 1-46 *show ospfv3 interface Field Descriptions*

Field	Description
Ethernet	Status of physical link and operational status of protocol.
IPv6 Address	Interface IPv6 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 of timer intervals.
Hello	Number of seconds until next hello packet is sent out this interface.

Send document comments to nexus7k-docfeedback@cisco.com

show ospfv3 memory

To display the memory usage statistics for the Open Shortest Path First version 3 (OSPFv3) protocol, use the **show ospfv3 memory** command.

show [ipv6] ospfv3 memory

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command requires the Enterprise Services license.

Examples	This example shows how to display the memory statistics for OSPFv3:

```
Router# show ospfv3 memory
OSPFv3 Process ID sd, Memory statistics
Process memory: 2096 KB
Byte usage:      needed 0, overhead 192, using 192 bytes
Allocations:     current 6, created 6, failed 0, free 0
Bitfields:       current 30, created 30, failed 0, free 0, using 248010 bytes
Slabs:           current 2, created 2, failed 0, free 0, using 80 bytes
Index failure:   Interface 0, Neighbor 0

Slab Memory
OSPFv3 vertex slab
Alloc 1, max allocs 1, total allocs 1, total frees 0
Total block allocs 1, total block frees 0, max blocks 1
Bytes (size/allocated) 68/69720
OSPFv3 IPv4 prefix routes slab
Alloc 0, max allocs 0, total allocs 0, total frees 0
Total block allocs 0, total block frees 0, max blocks 0
Bytes (size/allocated) 188/64
OSPFv3 router routes slab
Alloc 0, max allocs 0, total allocs 0, total frees 0
Total block allocs 0, total block frees 0, max blocks 0
Bytes (size/allocated) 100/64
OSPFv3 IPv4 next-hops slab
```

 show ospfv3 memory

Send document comments to nexus7k-docfeedback@cisco.com

```
Alloc 1, max allocs 1, total allocs 1, total frees 0
Total block allocs 1, total block frees 0, max blocks 1
Bytes (size/allocated) 32/262232
```

Table 1-18 describes the significant fields shown in the displays.

Table 1-47 *show ospfv3 memory Field Descriptions*

Field	Description

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 neighbors

To display Open Shortest Path First version 3 (OSPFv3)-neighbor information on a per-interface basis, use the **show ospfv3 neighbor** command.

```
show [ipv6] ospfv3 [instance-tag] neighbors [interface-type interface-number] [neighbor-id]
[detail] [summary] [vrf vrf-name]
```

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
<i>area-id</i>	(Optional) Area number used to define the particular area. Specify as an IP address or a number from 0 to 4294967295.
<i>interface-type</i>	(Optional) Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
<i>interface-number</i>	(Optional) Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.
<i>neighbor-id</i>	(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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the show ospfv3 neighbors command to display information about all or some of the neighbors for this OSPFv3 instance.

This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to display the summary information about the neighbor that matches the neighbor ID:

```
Router# show ospfv3 neighbors
OSPFv3 Process ID p1 vrf Red
Total number of neighbors: 2
Neighbor ID      Pri State           Up Time   Interface ID  Interface
60.60.60.60      1 FULL/DR          2d03h    5             GigE2/0/5
Neighbor address fe80::0206:d6ff:fec8:a41c
60.60.60.60      1 FULL/DR          2d03h    4             GigE2/0/6
Neighbor address fe80::0206:d6ff:fec8:a408
```

[Table 1-18](#) describes the significant fields shown in the displays.

Table 1-48 *show ospfv3 neighbors Field Descriptions*

Field	Description
Neighbor ID	Neighbor router ID.
Pri State	OSPFv3 priority and state.
Up Time	Time since the OSPFv3 established adjacency with this neighbor.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 policy statistics area

To display Open Shortest Path First version 3 (OSPFv3) policy statistics for an area, use the **show ospfv3 policy statistics area** command.

show [**ipv6**] **ospfv3** [*instance-tag*] **policy statistics area** *area id* **filter-list** {**in** | **out**} [**vrf** *vrf-name*]

Syntax Description	<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
	area <i>area-id</i>	Specifies the area number used to define the particular area. Specify as an IP address or a number from 0 to 4294967295.
	filter-list	Filters prefixes between OSPFv3 areas.
	in	Displays policy statistics for incoming routes.
	out	Displays policy statistics for outgoing routes.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Use the **show ospfv3 policy statistics area** command to display information about the filter lists applied to an area.

This command requires the Enterprise Services license.

Examples

This example shows how to display policy statistics for OSPFv3:

```
switch# show ospfv3 policy statistics area
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 policy statistics redistribute

To display Open Shortest Path First version 3 (OSPFv3) policy statistics, use the **show ospfv3 policy statistics redistribute** command.

```
show [ipv6] ospfv3 [instance-tag] policy statistics redistribute {bgp id | direct | isis id | rip id |
static} [vrf vrf-name]
```

Syntax Description	
<i>instance-tag</i>	(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.
isis	Displays policy statistics for the Intermediate-System to Intermediate-System (IS-IS) routing protocol.
rip	Displays policy statistics for the Routing Information Protocol (RIP).
static	Displays policy statistics for IP static routes.
<i>id</i>	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 isis 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 NX-OS stores it internally as a string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the show ospfv3 policy statistics redistribute command to display redistribution statistics. This command requires the Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to display policy statistics for redistributed routes:

```
switch# show ospfv3 policy statistics redistribute
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ospfv3 request-list** command.

show [**ipv6**] **ospfv3 request-list** *neighbor-id* *interface* *interface-number*

Syntax Description

<i>neighbor-id</i>	Router ID of the neighbor. Specify as an IP address.
<i>interface-type</i>	Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
<i>interface-number</i>	Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show ospfv3 request-list** command to troubleshoot Open Shortest Path First version 3 (OSPFv3) routing operations.

This command requires the Enterprise Services license.

Examples

This example shows how to display a list of all LSAs requested by a router:

```
Router# show ospfv3 request-list 40.40.40 ethernet 2/1
OSPFv3 Process ID p1
Neighbor 40.40.40.40, interface Ethernet2/1, address 192.0.2.1
1 LSAs on request-list

Type  LS ID          ADV RTR          Seq NO          Age          Checksum
1   192.0.2.12      192.0.2.12      0x8000020D      8           0x6572
```

Table 1-19 describes the significant fields shown in the displays.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-49 *show ospfv3 request-list Field Descriptions*

Field	Description
Type	LSA type.
LS ID	IP address of the neighbor router.
ADV RTR	IP address of the advertising router.
Seq NO	Packet sequence number of the LSA.
Age	Age, in seconds, of the LSA.
Checksum	Checksum number of the LSA.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be resent to neighbors, use the **show ospfv3 retransmission-list** command.

show [**ipv6**] **ospfv3 retransmission-list** *neighbor-id interface interface-number*

Syntax Description

<i>neighbor-id</i>	Router ID of the neighbor. Specify as an IP address.
<i>interface-type</i>	Interface type. If the <i>interface-type</i> argument is included, only information for the specified interface type is included. Type ? on the CLI for help on available options for this argument.
<i>interface-number</i>	Interface number. If the <i>interface-number</i> argument is included, only information for the specified interface number is included. Type ? on the CLI for help on available options for this argument.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show ospfv3 retransmission-list** command to troubleshoot Open Shortest Path First version 3 (OSPFv3) routing operations.

This command requires the Enterprise Services license.

Examples

This example shows how to display all LSAs waiting to be resent to neighbors:

```
Router# show ospfv3 retransmission-list 192.0.2.11 ethernet 2/1

      OSPFv3 Router with ID (192.0.2.12) (Process ID 1)

Neighbor 192.0.2.11, interface Ethernet2/1 address 209.165.201.11
Link state retransmission due in 3764 msec, Queue length 2

Type  LS ID          ADV RTR          Seq NO          Age          Checksum
  1   192.0.2.12      192.0.2.12      0x80000210      0           0xB196
```

Table 1-20 describes the significant fields shown in the displays.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-50 ***show ospfv3 retransmission-list Field Descriptions***

Field	Description
Type	LSA type.
LS ID	IP address of the neighbor router.
ADV RTR	IP address of the advertising router.
Seq NO	Packet sequence number of the LSA.
Age	Age, in seconds, of the LSA.
Checksum	Checksum number of the LSA.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 routes

To display the Open Shortest Path First version 3 (OSPFv3) topology table, use the **show ospfv3 routes** command.

show [**ipv6**] **ospfv3** [*instance-tag*] **routes** [*prefix/length* | **summary**] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
<i>prefix /length</i>	(Optional) IP prefix, which limits output to a specific route. Indicate the length as a slash (/) and number from 1 to 255. 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 <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show ospfv3 routes** command to display the OSPFv3 private routing table (which contains only routes that are calculated by OSPFv3). If something is wrong with a route in the routing information base (RIB), then you should check the OSPFv3 copy of the route to determine if it matches the RIB contents. If it does not match, a synchronization problem exists between OSPFv3 and the RIB.

This command requires the Enterprise Services license.

Examples

This example shows how to display OSPFv3 routes:

```
RP/0/RP0/CPU0:router# show ospfv3 routes
OSPFv3 routing table
1111:1111::/32 (i) area 0
    via directly connected
1111:2222::/32 (i) area 1
    via directly connected
```

Send document comments to nexus7k-docfeedback@cisco.com

```
1111:4444::0001/128 (i) area 0
    via directly connected
1111:5555::/32 (i) area 0
1111:6666::/32 (i) area 1
    via directly connected
6060:6060::6060/128 (i) area 0
    via fe80::0206:d6ff:fec8:a41c/Enet2/5, cost 10
6161:6161::6161/128 (i) area 1
    via fe80::0206:d6ff:fec8:a408/Enet2/6, cost 10
```

Table 1-21 describes the significant fields shown in the display.

Table 1-51 *show ospfv3 route Field Descriptions*

Field	Description
1111:1111::/32	Router ID for the router that advertised this route.
via...	Packets destined for the given prefix are sent over the listed interface or directly connected to this device.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 statistics

To display Open Shortest Path First version 3 (OSPFv3) shortest path first (SPF) calculation statistics, use the **show ospfv3 statistics** command.

show [**ipv6**] **ospfv3** [*instance-tag*] **statistics** [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show ospfv3 statistics** command to display information about link-state advertisements (LSAs). This information can be useful for both OSPFv3 network maintenance and troubleshooting. For example, we recommend that you use the **show ospfv3 statistics** command as the first troubleshooting step for LSA flapping.

This command requires the Enterprise Services license.

Examples

This example shows how to display information about the SPF calculations:

```
Router# show ospfv3 statistics
OSPFv3 Process p1 vrf default, Event statistics (cleared 2w3d ago)
```

```
Router ID changes: 0
DR elections: 5
Older LSAs received: 0
Neighbor state changes: 10
Neighbor dead postponed: 0
Neighbor dead interval expirations: 0
Neighbor bad lsregs: 0
Neighbor sequence number mismatches: 0
SPF computations: 9 full, 0 summary, 0 external
```

Send document comments to nexus7k-docfeedback@cisco.com

LSA Type	Generated	Refreshed	Flushed	Aged out
Router	4	202	0	0
Network	0	0	0	0
Inter-Area-Prefix	0	606	7	0
Inter-Area-Router	0	0	0	0
AS External	0	0	0	0
Link-Local	7	505	0	0
Intra-Area-Prefix	6	202	0	0
Unknown	0	0	0	0

Following counters can not be reset:

LSA deletions: 0 pending, 2 hwm, 16 deleted, 0 revived, 2 runs
 Hello queue: 0/200, hwm 2, drops 0
 Flood queue: 0/100, hwm 2, drops 0
 LSDB additions failed: 0

Buffers:	in use	hwm	permanent	alloc	free
128 bytes	0	2	1	142512	142512
512 bytes	0	2	2	779	779
1520 bytes	0	1	0	1	1
4500 bytes	0	1	1	891	891
huge	0	0	0	0	0

Table 1-22 describes the significant fields shown in the display.

Table 1-52 *show ospfv3 statistics Field Descriptions*

Field	Description
OSPFv3 process	Unique value assigned to the OSPFv3 instance in the configuration.
vrf	Virtual routing and forwarding (VRF) for this OSPFv3 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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 summary-address

To display a list of all summary address redistribution information configured in an Open Shortest Path First version 3 (OSPFv3) instance, use the **show ospfv3 summary-address** command.

show [**ipv6**] **ospfv3** [*instance-tag*] **summary-address** [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to display information about summary addresses:

```
Router# show ospfv3 summary-address
```

```
OSPFv3 Router with ID (40.40.40.40) (Process ID p1Configured summary-address
```

```
2000::/8 Pending
6161::/16 Pending
```

[Table 1-18](#) describes the significant fields shown in the displays.

Table 1-53 *show ospfv3 summary-address Field Descriptions*

Field	Description
10.2.0.0/255.255.0.0	IP address and mask of the router for the OSPFv3 process.
Metric -1	OSPFv3 metric type.

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-53 *show ospfv3 summary-address Field Descriptions (continued)*

Field	Description
Type 0	Type of LSA.
Tag 0	OSPFv3 process tag identifier.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 traffic

To display Open Shortest Path First version 3 (OSPFv3) traffic statistics, use the **show ospfv3 traffic** command.

show [**ipv6**] **ospfv3** [*instance-tag*] **traffic** [**vrf** *vrf-name*]

Syntax Description	
<i>instance-tag</i>	(Optional) Name of the OSPF instance. Specify as an alphanumeric string.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults	None

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the show ospfv3 traffic command to display traffic statistics for one or more OSPFv3 instances. This command requires the Enterprise Services license.

Examples	This example shows how to display OSPFv3 traffic statistics:

```
Router# show ospfv3 traffic
```

```
OSPFv3 Process ID p1, vrf Red, Packet Counters (cleared 2w3d ago)
Total: 1690 in, 349230 out
LSU transmissions: first 100, rxmit 108, for req 16
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, unknown in    0, unknown out    0
      no ospfv3      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, nbr changed rid/ip addr 0
      bad auth       0
```


Send document comments to nexus7k-docfeedback@cisco.com

```

                hellos      dbds      lsreqs      lsus      acks
In:             1411        70         16         136       57
Out:            348871      62          4         224       69

```

Table 1-24 describes the significant fields shown in the display.

Table 1-54 *show ospfv3 traffic Field Descriptions*

Field	Description
OSPFv3 Process	OSPFv3 instance tag for these traffic statistics.
vrf	Virtual routing and forwarding (VRF) for this OSPFv3 instance.
Errors	
drops	Number of packets dropped.
bad version	Number of packets received with bad version.
dup rid	Number of packets with a duplicate router-id
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)
lsacks	Number of packets of type LSACK (LSA acknowledged)

Related Commands

Command	Description
clear ipv6 ospfv3 traffic	Clears OSPFv3 traffic statistics.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show ospfv3 virtual-links

To display parameters and the current state of Open Shortest Path First version 3 (OSPFv3) virtual links, use the **show ospfv3 virtual-links** command.

show [**ipv6**] **ospfv3** [*instance-tag*] **virtual-links** [**brief**] [**vrf** *vrf-name*]

Syntax Description

<i>instance-tag</i>	(Optional) Name of the OSPF instance. Use this tag to display OSPFv3 information about a specific OSPFv3 instance.
brief	(Optional) Displays a summary of the configured virtual links.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as any case-insensitive alphanumeric string up to 32 characters. The strings “default” and “all” are reserved VRF names.

Defaults

None

Command Modes

Any

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show ospfv3 virtual-links** command to display information about configured virtual links. This command requires the Enterprise Services license.

Examples

This example shows how to display information about virtual links:

```
Router# show ospfv3 virtual-links
```

```
Virtual link 2 to router 40.40.40.40 is up
  Process ID pl vrf default, Transit area 1, via interface Ethernet1/2, cost 10
  Transit area 33, remote addr 0::
  IPv6 address 0::
  Process ID sd vrf default, Instance ID 0, area 0
  State DOWN, Network type P2P, cost 65535
  Index 1, Transmit delay 1 sec
  0 Neighbors, flooding to 0, adjacent with 0
  Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
  Number of link LSAs: 0, checksum sum 0
  Adjacency Information
```

Send document comments to nexus7k-docfeedback@cisco.com

Table 1-25 describes the significant fields shown in the display.

Table 1-55 ***show ospfv3 virtual-links Field Descriptions***

Field	Description
Virtual Link	OSPFv3 neighbor and whether the link to that neighbor is up or down.
vrf	Virtual routing and forwarding (VRF) for this OSPFv3 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 OSPFv3 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 timer due in 0:00:04	Time when the next hello is expected from the neighbor.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show routing

To display routing information, use the **show routing** command.

show routing [**ip** | **ipv4** | **ipv6**] [*address* | *hostname* | *prefix* | *route-type* | **clients** | **hidden-nh** | **interface** *type number* | **next-hop** *addr* | **recursive-next-hop** [*addr*]] [**vrf** *vrf-name*]

Syntax Description		
<i>address</i>	(Optional) IPv4 or IPv6 address. IPv4 address format is x.x.x.x. IPv6 address format is A:B::C:D.	
<i>hostname</i>	Host name. The <i>name</i> can be any case-sensitive alphanumeric string up to 80 characters.	
<i>prefix</i>	(Optional) IPv4 or IPv6 prefix. IPv4 prefix format is x.x.x.x/length. IPv6 address format is A:B::C:D/length.	
<i>route-type</i>	(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 <i>type number</i>	(Optional) Displays the routes for an interface. Use ? to see the supported interfaces.	
next-hop <i>addr</i>	(Optional) Displays routes with this next-hop address. The format is x.x.x.x.	
recursive next-hop <i>addr</i>	(Optional) Displays routes with this recursive next-hop address. The format is x.x.x.x.	
vrf <i>vrf-name</i>	(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

Supported User Roles network-admin
network-operator
vdc-admin
vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Added <i>hostname</i> argument.
	4.2(1)	Added hidden-nh keyword.

Usage Guidelines This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example displays the route table:

```
switch(config)# show ip routing
IP Route Table for VRF "default"
'*' denotes best ucast next-hop      '*' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

0.0.0.0/32, 1 ucast next-hops, 0 mcast next-hops
    *via Null0, [220/0], 00:45:24, local, discard
255.255.255.255/32, 1 ucast next-hops, 0 mcast next-hops
    *via sup-eth1, [0/0], 00:45:24, local
```

Related Commands

Command	Description
clear ip route	Clears entries in the route table.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

show routing memory estimate

To display an estimate of routing memory requirements, use the **show routing memory estimate** command.

show routing memory estimate *num-routes***|next-hops** *num-hop-addresses*

Syntax Description

<i>num-routes</i>	Number of routes. The range is from 1000 to 112000.
<i>num-hop-addresses</i>	Number of next-hop addresses per route. The range is from 1 to 16.

Defaults

None

Command Modes

Any command mode

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(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.

This command does not require a license.

Examples

This example displays the route table:

```
switch# show routing memory estimate routes 110000 next-hops 16
Shared memory estimates:
  Current max      32 MB;  26125 routes with 16 nhs
    in-use       1 MB;    11 routes with  1 nhs (average)
  Configured max   32 MB;  26125 routes with 16 nhs
  Estimate        135 MB; 110000 routes with 16 nhs
```

Send document comments to nexus7k-docfeedback@cisco.com

show routing-context

To display the virtual routing and forwarding (VRF) scope for all EXEC commands, use the **show routing-context** command.

show routing-context

Syntax Description	This command has no keywords or arguments.

Defaults	None

Command Modes	EXEC

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows how display the current routing context: <pre>switch#management# show routing-context Current Route Context: management</pre>

Related Commands	Command	Description
	routing-context vrf	Configures the routing context.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>source-addr</i>	Source IPv4 address. IPv4 address format is x.x.x.x.
<i>dest-addr</i>	Destination IPv4 address. IPv4 address format is x.x.x.x.
<i>source-port</i>	(Optional) Source port. The range is from 1 to 65535.
<i>dest-port</i>	(Optional) Destination port. The range is from 1 to 65535.
vrf <i>vrf-name</i>	(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

Supported User Roles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the route selected to reach 30.0.0.2 from 10.0.0.2:

```
switch# show routing hash 10.0.0.5 30.0.0.2
Load-share parameters used for software forwarding:
load-share mode: address source-destination port source-destination
Universal-id seed: 0xe05e2e85
Hash for VRF "default"
Hashing to path *20.0.0.2 (hash: 0x0e), for route:
```

Related Commands

Command	Description
clear ip route	Clears entries in the route table.

Send document comments to nexus7k-docfeedback@cisco.com

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 <i>id</i> 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.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example shows how to display the UDP socket client information:

```
switch# show socket client udp
Total number of UDP clients: 8

client: syslogd, pid: 3307, sockets: 1
client: ntp, pid: 3577, sockets: 2
client: ntpd, pid: 3660, sockets: 3
client: snmpd, pid: 3579, sockets: 2
client: hsrp_engine, pid: 3786, sockets: 2
client: pim, pid: 3782, sockets: 1
client: glbp, pid: 3783, sockets: 1
client: radiusd, pid: 3572, sockets: 2
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

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 <i>id</i> range is from 1 to 65535.
	local address	(Optional) Displays information about all the TCP connections with the specified local address. The <i>address</i> can be an IPv4 or an IPv6 address.
	foreign address	(Optional) Displays information about all the TCP connections with the specified foreign address. The <i>address</i> can be an IPv4 or an IPv6 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.

Defaults	None

Command Modes	Any command mode

Supported User Roles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example shows how to display the TCP socket connection information:

```
switch# show socketx connection tcp
Total number of tcp sockets: 10
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)
```

Send document comments to nexus7k-docfeedback@cisco.com

	Wildcard	0	* (*)
tcp	LISTEN	0	*(161)
	Wildcard	0	* (*)
tcp6	LISTEN	0	*(161)
	Wildcard	0	* (*)
tcp	LISTEN	0	*(179)
	Wildcard	0	* (*)
tcp6	LISTEN	0	*(179)
	Wildcard	0	* (*)
tcp	ESTABLISHED	0	172.28.230.85(22)
	management	0	172.28.254.254(1055)
tcp	ESTABLISHED	0	172.28.230.85(22)
	management	0	172.28.254.254(3353)
tcp	ESTABLISHED	0	172.28.230.85(23)
	management	0	10.82.232.102(2390)
tcp	ESTABLISHED	0	172.28.230.85(23)
	management	4	161.44.67.127(1242)

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.

Send document comments to nexus7k-docfeedback@cisco.com

show sockets statistics

To display the socket statistics, use the **show sockets statistics** command.

show sockets statistics [**all** | **raw** | **raw6** | **rawsum** | **tcp** | **tcp6** | **tcpsum** | **udp** | **udp6** | **udpsum**]

Syntax Description	
all	(Optional) Displays all the socket statistics.
raw	(Optional) Displays the socket statistics for the raw IPv4 protocol socket statistics.
raw6	(Optional) Displays the socket statistics for the raw IPv6 protocol socket statistics.
rawsum	(Optional) Displays a summary of the socket statistics for the raw IPv4 and IPv6 protocol socket statistics.
tcp	(Optional) Displays the socket statistics for the TCP IPv4 protocol.
tcp6	(Optional) Displays the socket statistics for the TCP IPv6 protocol.
tcpsum	(Optional) Displays a summary of the socket statistics for the TCP IPv4 and IPv6 protocols.
udp	(Optional) Displays the socket statistics for the UDP IPv4 protocol.
udp6	(Optional) Displays the socket statistics for the UDP IPv6 protocol.
udpsum	(Optional) Displays a summary of the socket statistics for the UDP IPv4 and IPv6 protocols.

Defaults	None

Command Modes	Any command mode

SupportedUserRoles	network-admin network-operator vdc-admin vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	The following example shows how to display the TCP socket statistics:

```
switch# show sockets statistics tcp
TCP v4 Received:
  36490 packets total
  0 checksum error, 0 bad offset, 0 too short, 0 MD5 error
```

Send document comments to nexus7k-docfeedback@cisco.com

```

18711 packets (950071 bytes) in sequence
2 duplicate packets (136 bytes)
0 partially dup packets (0 bytes)
1 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
17 duplicate ack packets, 0 ack packets with unsent data
26130 ack packets (8137813 bytes)
TCP v4 Sent:
44602 total, 0 urgent packets
6 control packets
43908 data packets (8137790 bytes)
0 data packets (0 bytes) retransmitted
688 ack only packets
0 window probe packets, 0 window update packets
TCP v4:
0 connections initiated, 21 connections accepted, 21 connections established
18 connections closed (including 11 dropped, 0 embryonic dropped)
0 total rxmt timeout, 0 connections dropped in rxmt timeout
12 keepalive timeout, 12 keepalive probe, 0 connections dropped in keepalive

```

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.

Send document comments to nexus7k-docfeedback@cisco.com

show track

To show information about object tracking, use the **show track** command.

```
show track [object-id] [interface | { ip | ipv6 } route] [brief]
```

Syntax Description	<i>object-id</i>	(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.
	ipv6 route	(Optional) Displays information about tracked IPv6 routes.
	brief	(Optional) Displays brief information about tracked objects.

Defaults	Display information for all tracked objects.

Command Modes	Any

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	Added ipv6 keyword
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.

Examples	This example shows how to display information about tracked interfaces:

```
switch# show track interface
Track 1
  Interface Ethernet1/2 IP Routing
  IP Routing is DOWN
  1 changes, last change 00:35:14

Track 2
  Interface Ethernet2/2 Line Protocol
  Line Protocol is DOWN
  1 changes, last change 00:33:55

Track 4
  Interface Ethernet2/45 IP Routing
  IP Routing is DOWN
  1 changes, last change 00:17:03
```

Send document comments to nexus7k-docfeedback@cisco.com

```
Track 6
  Interface Ethernet2/34 Line Protocol
  Line Protocol is DOWN
  1 changes, last change 00:15:12
```

This example shows how to display information about tracked IP routes:

```
switch# show track ip route
Track 3
  IP Route 10.10.10.0/8 Reachability
  Reachability is DOWN
  1 changes, last change 00:22:09
```

This example shows how to display brief information about tracked objects:

```
switch# show track brief
Track Type      Instance      Parameter      State  Last Change
1    Interface  Ethernet1/2    IP Routing     DOWN   00:36:42
2    Interface  Ethernet2/2    Line Protocol  DOWN   00:35:22
3    IP Route   10.10.10.0/8   Reachability   DOWN   00:22:47
4    Interface  Ethernet2/45   IP Routing     DOWN   00:18:31
6    Interface  Ethernet2/34   Line Protocol  DOWN   00:16:40
switch#
```

Related Commands

Command	Description
track interface	Tracks the state of an interface.
track ip route	Tracks the state of an IP route.
track ipv6 route	Tracks the state of an IPv6 route.

Send document comments to nexus7k-docfeedback@cisco.com

show vrrp

To show information about the Virtual Router Redundancy Protocol (VRRP), use the **show vrrp** command.

show vrrp [**detail** | **statistics**] [**interface** *if-number*] [**vr** *id*] [**master** | **backup** | **init**]

Syntax Description	detail	(Optional) Displays detailed information about VRRP.
	statistics	(Optional) Displays VRRP statistics.
	interface <i>if-number</i>	(Optional) Displays information about VRRP on an interface. Use ? to see a list of supported interfaces.
	vr <i>id</i>	(Optional) Displays information about VRRP for a group. The <i>id</i> range is from 1 to 255.
	master	(Optional) Displays information about VRRP groups in the master state.
	backup	(Optional) Displays information about VRRP groups in the backup state.
	init	(Optional) Displays information about VRRP groups in the init state.

Defaults Display information for all VRRP groups.

Command Modes Any

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display information about VRRP:

```
switch(config)# show vrrp
      Interface  VR  IpVersion  Pri    Time  Pre  State  VR  IP  addr
-----
      Ethernet7/45  33   IPV4       100    1 s   Y    Init
      Ethernet7/45  99   IPV4       100    1 s   Y    Init
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
feature vrrp	Enables the VRRP feature.
clear vrrp	Clears VRRP statistics.



T Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter T.

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	<i>peer name</i>	Specifies the name of the neighbor template.
	<i>peer-policy name</i>	Specifies the name of the peer-policy template.
	<i>peer-session name</i>	Specifies the name of the peer-session template.

Command Default	This command has no default settings.

Command Modes	Neighbor address-family configuration Router bgp configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	The template command allows you to enable a set of predefined attributes that a neighbor inherits.

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

A 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.

Peer Templates

The peer template combines the peer-session and peer-policy templates to form a basic neighbor definition. It is not mandatory to use a neighbor template but you can use it to simplify the BGP configuration.

Peer-policy Templates

Peer-policy templates are used to group and apply the configuration of commands that are applied within specific address-families and NLRI configuration mode. Peer-policy templates are created and configured in peer policy configuration mode. BGP policy commands that are configured for specific address-families or NLRI configuration modes are configured in a peer-policy template. 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.
- **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 will overwrite 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.

Send document comments to nexus7k-docfeedback@cisco.com

- **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 nexthop if possible.
- **no**—Negates a command or set 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, thus preventing 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 will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

- **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 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 is displayed:

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 will inherit the characteristic configured with this command.

Send document comments to nexus7k-docfeedback@cisco.com

Similar to peer-session templates, peer-policy templates are configured once and applied to many neighbors through the direct application of a peer-policy template or through inheritance from peer-policy templates. The configuration of peer-policy templates simplifies the configuration of BGP policy commands that are applied to all neighbors within an autonomous system.

Peer-policy templates support direct and indirect inheritance from up to eight 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 and ending with the highest sequence number. However, there is a difference; a peer-policy template will not fall through like a route-map. Every sequence is evaluated, and if a BGP policy command is reapplied with different value, it will overwrite any previous value from a lower sequence number.

Peer-policy 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-policy templates.



Note

A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies from only peer templates.

Peer-session Templates

Peer-session templates are used to group and apply the configuration of general session commands to groups of neighbors that share common session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer-session template. Peer-session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer-session template.

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:

Send document comments to nexus7k-docfeedback@cisco.com

- **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.
- **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.

Peer-session templates support direct and indirect inheritance. A peer can be configured with only one peer-session template at a time, and that peer-session template can contain only one indirectly inherited peer-session template. However, each inherited session template can also contain one indirectly inherited peer-session template. So, only one directly applied peer-session template and up to seven additional indirectly inherited peer-session templates can be applied, allowing you to apply up to a maximum of eight peer session configurations to a neighbor: the configuration from the directly inherited peer-session template and the configurations from up to seven indirectly inherited peer-session templates. Inherited peer-session templates are evaluated first, and the directly applied template will be evaluated and applied last. So, if a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template.

Peer-session templates support only general session commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer-policy templates.

This command requires the Enterprise Services license.

Examples

The following example creates a peer-session template named CORE1. This example inherits the configuration of the peer-session template named INTERNAL-BGP.

```
switch(config-router)# template peer-session CORE1
switch(config-router-stmp)#
```

The following example shows how to create and configure a peer-policy template named CUSTOMER-A:

```
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)#
```

Send document comments to nexus7k-docfeedback@cisco.com

The following example shows that the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

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

The following example shows that the maximum number of prefixes that will be 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(config)# router bgp 64496
switch(config-router) network 192.168.0.0
switch(config-router) # maximum-prefix 5000 50
```

The following example shows that the maximum number of prefixes that will be 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(config)# router bgp 64496
switch(config-router) network 192.168.0.0
switch(config-router) # neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

The following example shows that the warning messages is 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
```

The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
switch(config)# router bgp 64496
switch(config-router) # next-hop-self
```

The following router configuration mode example, 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(config)# router bgp 64496
switch(config-router) # send-community
```

The following address family configuration mode example, 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(config)# router bgp 64496
switch(config-router) # address-family ipv4 multicast
switch(config-router-af) # send-community
```

The following example enables inbound soft reconfiguration for the neighbor 10.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information will be used to generate a new set of inbound updates.

```
switch(config)# router bgp 64496
switch(config-router) # soft-reconfiguration inbound
```

Related Commands

Command	Description
router bgp	Enters the assign an autonomous system (AS) number to a router and enters the router BGP configuration mode
address-family	Enters the address family mode for the Border Gateway Protocol (BGP).

Send document comments to nexus7k-docfeedback@cisco.com

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 keywords or arguments.

Defaults

None

Command Modes

Any

Supported User Roles

Network Administrator
VDC Administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

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.

Send document comments to nexus7k-docfeedback@cisco.com

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** | **ipv6**] [**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.
ipv6	(Optional) Specifies the inconsistency check for IPv6 routes.
unicast	(Optional) Specifies the inconsistency check for unicast routes.
module	(Optional) Specifies the inconsistency check for one or more modules.
<i>slot</i>	Module number. The range depends on the platform.
all	(Optional) Specifies the inconsistency check for all modules.
stop	(Optional) Stops the inconsistency check.

Defaults

None

Command Modes

Any

Supported User Roles

Network Administrator
VDC Administrator

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added support for ipv6 keyword.

Usage Guidelines

This command does not require a license.

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

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
clear forwarding inconsistency	Clears the FIB inconsistencies.
show forwarding inconsistency	Displays information about the FIB inconsistencies.

Send document comments to nexus7k-docfeedback@cisco.com

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	Specifies the down threshold.
	<i>number</i>	Threshold value. The range is from 0 to 100.

Defaults	None

Command Modes	tracking configuration

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	When you configure a tracked list using the track <i>object-number</i> 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, then the weight keyword is unavailable. If you specify the weight keyword, then 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 will see a range from 0 to 49 percent for down. This command does not require a license.

Examples	In the following example, the tracked list 11 is configured 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
```

 threshold percentage

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

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	Specifies the down threshold.
	<i>number</i>	Threshold value. The range is from 1 to 255.

Defaults	None

Command Modes	tracking configuration

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines	When you configure a tracked list using the track <i>object-number</i> 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, then the weight keyword is unavailable. If you specify the weight keyword, then 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	In the following example, the tracked list 12 is configured 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
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

timers (GLBP)

To configure the time between hello packets sent by the Gateway Load Balancing Protocol (GLBP) gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **timers** command. To return the timers to the default values, use the **no** form of this command.

timers [**msec**] *hellotime* [**msec**] *holdtime*

no timers

Syntax Description	msec	(Optional) Specifies that the following (<i>hellotime</i> or <i>holdtime</i>) argument value will be expressed in milliseconds.
	<i>hellotime</i>	Hello interval. The range is from 1 to 60 seconds. The default is 3 seconds (3000 milliseconds).
	<i>holdtime</i>	Time before the virtual gateway and virtual forwarder information contained in the hello packet is considered invalid. The range is from 2 to 180 seconds. The default is 10 seconds (10,000 milliseconds).

Defaults	<i>hellotime</i> : 3 seconds <i>holdtime</i> : 10 seconds

Command Modes	GLBP configuration

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	If you do not configure timers on a gateway, the gateway learns the timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All gateways in a GLBP group should use the same timer values. If a GLBP gateway sends a hello message, the information should be considered valid for one holdtime. Typically, the holdtime is greater than three times the value of the hello time, (<i>holdtime</i> > 3 * <i>hellotime</i>). The range of values for the holdtime force the holdtime to be greater than the hello time.

This command does not require a license.

Examples	This example shows how to configure the timers for GLBP group 10 on Ethernet interface 1/1:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# timers 5 18
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
timers redirect	Configures the redirect and timeout values for the GLBP group.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>time-limit</i>	(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.
Defaults	Disabled	
Command Modes	Address family configuration Router configuration Router VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following 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	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

timers basic

To adjust the Routing Information Protocol (RIP) network timers, use the **timers basic** command in router address-family configuration mode. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush*

no timers basic

Syntax Description		
<i>update</i>		Rate (in seconds) at which updates are sent. The default is 30 seconds.
<i>invalid</i>		Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when no updates refresh the route. The route then enters into a <i>holddown</i> state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. The default is 180 seconds.
<i>holddown</i>		Interval (in seconds) during which routing information regarding better paths is suppressed; it should be at least three times the value of the <i>update</i> argument. A route enters into a <i>holddown</i> 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 default is 180 seconds.
<i>flush</i>		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 <i>invalid</i> argument plus the <i>holddown</i> argument. If it is less than this sum, the proper <i>holddown</i> interval cannot elapse, which results in a new route being accepted before the <i>holddown</i> interval expires. The default is 240 seconds.

Defaults

update: 30 seconds
invalid: 180 seconds
holddown: 180 seconds
flush: 240 seconds

Command Modes

Router address-family configuration

Command History

Release	Modification
4.0(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.

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

You can view the current and default timer values by using the **show ip protocols** command.

This command does not require a license.

Examples

The following example shows how to set updates to broadcast every 5 seconds. If Cisco NX-OS does not hear from a router in 15 seconds (the invalid time), it declares the route as unusable. Cisco NX-OS suppresses further information for an additional 15 seconds (the holddown time). At the end of the suppression period, Cisco NX-OS 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
```

Related Commands

Command	Description
address-family	Enters address-family configuration mode.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>milliseconds</i>	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.

Defaults	1000 milliseconds

Command Modes	Router configuration VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	The following 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
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show ip ospf timers rate-limit	Displays all of the LSAs in the rate-limit queue.
	timers throttle lsa	Sets rate-limiting values for LSAs being generated.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

timers lsa-arrival (OSPFv3)

To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First version 3 (OSPFv3) 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	<i>milliseconds</i>	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.

Defaults	1000 milliseconds

Command Modes	Router configuration VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:
	<pre>switch(config)# router ospfv3 1 switch(config-router)# timers lsa-arrival 2000</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show ospfv3 timers rate-limit	Displays all of the LSAs in the rate-limit queue.
	timers throttle lsa	Sets rate-limiting values for LSAs being generated.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>seconds</i>	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.

Defaults

The default interval for this command is 240 seconds. OSPF LSA group pacing is enabled by default.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 NX-OS 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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following 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  
switch(config-router)# timers lsa-group-pacing 60
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

timers lsa-group-pacing (OSPFv3)

To change the interval at which Open Shortest Path First version 3 (OSPFv3) 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

<i>seconds</i>	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.

Defaults

The default interval for this command is 240 seconds. OSPFv3 LSA group pacing is enabled by default.

Command Modes

Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless you have tried all other options to meet OSPFv3 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 OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Cisco NX-OS 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 Enterprise Services license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure OSPFv3 group packet-pacing updates between LSA groups to occur in 60-second intervals for OSPFv3 routing process 1:

```
switch(config)# router ospfv3 1  
switch(config-router)# timers lsa-group-pacing 60
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPFv3 routing processes.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>seconds</i>	Time limit for convergence after an NSF switchover (in seconds). The range is from 60 to 180 seconds. The default value is 120.

Defaults

120 seconds

Command Modes

Address family configuration
Router configuration
Router VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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
```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>seconds</i> Time, in seconds, that EIGRP holds routes for an inactive peer. The range is from 20 to 300 seconds. The default is 240.	
Defaults	EIGRP NSF awareness is enabled. <i>seconds</i> : 240	
Command Modes	Address family configuration Router configuration Router VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 Enterprise Services license.	
Examples	The following example shows how to set the route hold timer value for an NSF-aware router to 2 minutes (120 seconds): <pre>switch(config)# router eigrp 1 switch(config-router) address-family ipv4 unicast switch(config-router-af)# timers nsf route-hold 120</pre>	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>seconds</i>	Time, in seconds, that EIGRP waits for a peer to signal an NSF restart. The range is from 10 to 30 seconds. The default is 20.

Defaults

EIGRP NSF awareness is enabled.
seconds: 20

Command Modes

Address family configuration
 Router configuration
 Router VRF configuration

Supported User Roles

network-admin
 vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

The following 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
```


[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

timers redirect

To configure the time interval in which the active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group continues to redirect clients to a secondary active virtual forwarder (AVF), use the **timers redirect** command. To return the redirect timers to the default values, use the **no** form of this command.

timers redirect *redirect timeout*

no timers redirect *redirect timeout*

Syntax Description	<i>redirect</i>	Redirect timer interval, in seconds. The range is from 0 to 3600 seconds. The default is 300 seconds (5 minutes).
	<i>timeout</i>	Time, in seconds, before the secondary virtual forwarder becomes unavailable. The range is from 610 to 64800 seconds. The default is 14,400 seconds (4 hours).

Defaults

redirect: 300 seconds
timeout: 14,400 seconds

Command Modes

GLBP configuration

Supported User Roles

Network Administrator
VDC Administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A virtual forwarder that is assigned a virtual MAC address by the AVG is referred to as a primary virtual forwarder. If the virtual forwarder learned the virtual MAC address from hello messages, it is referred to as a secondary virtual forwarder.

You can use the redirect timer to set a time delay that starts when a forwarder fails on the network and the AVG assumes that the forwarder will not return. When you set a time delay, the virtual MAC address that the forwarder replies to is still in the Address Resolution Protocol (ARP) replies, but the actual forwarding task is handled by another group in the GLBP group.

The timeout interval is the time delay that begins when a forwarder fails on the network and the MAC address that the forwarder was responsible for becomes inactive on all of the routers in the GLBP group. After the timeout interval, packets sent to this virtual MAC address will be lost. You must configure a timeout interval that is long enough to allow all hosts to refresh the ARP cache entry that contained the virtual MAC address.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to configure the redirect and timeout values for GLBP group 1 on Ethernet interface 1/1:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# timers redirect 600 7200
switch(config-glbp)# ip
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
timers	Configures hello and hold timers for GLBP.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>start-time</i>	Start time (in milliseconds) that is used to calculate the subsequent rate limiting times for LSA generation. The range is from 50 to 5000 milliseconds. The default value is 50 milliseconds.
	<i>hold-interval</i>	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.
	<i>max-time</i>	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.

Defaults	<i>start-time</i> : 50 milliseconds
	<i>hold-interval</i> : 5000 milliseconds
	<i>max-time</i> : 5000 milliseconds

Command Modes	Router configuration
	VRF configuration

Supported User Roles	network-admin
	vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.2(1)	Added <i>start-time</i> and <i>max-time</i> arguments.

Usage Guidelines	Use the timers throttle lsa command to rate-limit LSA generation.
	This command requires the Enterprise Services license.

Examples	This example shows how to customize OSPF LSA throttling:
	<pre>switch(config)# router ospf 1</pre>
	<pre>switch(config-router)# timers throttle lsa 50 5000 6000</pre>

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

timers throttle lsa (OSPFv3)

To set rate-limiting values for Open Shortest Path First version 3 (OSPFv3) 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	<i>start-time</i>	Start time (in milliseconds) that is used to calculate the subsequent rate limiting times for LSA generation. The range is from 50 to 5000 milliseconds. The default value is 50 milliseconds.
	<i>hold-interval</i>	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.
	<i>max-time</i>	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.

Defaults	<i>hold-interval</i> : 5000 milliseconds

Command Modes	Router configuration VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.2(1)	Added <i>start-time</i> and <i>max-time</i> arguments.

Usage Guidelines	Use the timers throttle lsa command to rate-limit LSA generation. This command requires the Enterprise Services license.

Examples	This example shows how to customize OSPFv3 LSA throttling: switch(config)# router ospfv3 1 switch(config-router)# timers throttle lsa 50 10000 5000

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
show ospfv3	Displays information about OSPFv3 routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPFv3 neighbors.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>spf-start</i>	Initial SPF schedule delay in milliseconds. The range is from 1 to 600000 milliseconds.
	<i>spf-hold</i>	Minimum hold time between two consecutive SPF calculations. the range is from 1 to 600000 milliseconds.
	<i>spf-max-wait</i>	Maximum wait time between two consecutive SPF calculations. The range is from 1 to 600000 milliseconds.
Defaults	SPF throttling is not set.	
Command Modes	Router configuration VRF configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(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 <i>spf-start</i> 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 <i>spf-maximum</i> argument. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.	
Examples	The following 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: <pre>switch(config)# router ospf 1 switch(config-router)# timers throttle spf 5 1000 90000</pre>	

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

timers throttle spf (OSPFv3)

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 version 3 (OSPFv3), 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

<i>spf-start</i>	Initial SPF schedule delay in milliseconds. The range is from 1 to 600000 milliseconds.
<i>spf-hold</i>	Minimum hold time between two consecutive SPF calculations. the range is from 1 to 600000 milliseconds.
<i>spf-max-wait</i>	Maximum wait time between two consecutive SPF calculations. The range is from 1 to 600000 milliseconds.

Defaults

SPF throttling is not set.

Command Modes

Address-family configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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 ospfv3 1
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# timers throttle spf 5 1000 90000
```


Send document comments to nexus7k-docfeedback@cisco.com

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 **track** *object-number* [**decrement** *value*]

Syntax Description	<i>object-number</i>	Number for a configured tracked object. The range is from 1 to 500.
	decrement <i>value</i>	(Optional) Decrements the VRRP priority if the tracked object is down. The range is from 1 to 254.

Defaults	None

Command Modes	VRRP configuration mode

Supported User Roles	network-admin VDC administrator

Command History	Release	Modified
	4.2(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.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to enable object tracking for a virtual router:

```
switch# config t
switch(config)# track 33 ip route 192.0.2.0/24 reachability
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# track 33 priority 2
```

Related Commands

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.
track interfave (VRRP)	Tracks the state of an interface and modifies the VRRP priority if that interface state goes down.

Send document comments to nexus7k-docfeedback@cisco.com

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** | **ipv6**} **routing** | **line-protocol**}

no track *object-id* [**force**]

Syntax Description	<i>object-id</i>	Tracking ID. The range can be from 1 to 500.
	interface <i>interface-type number</i>	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.
	ipv6 routing	Tracks the IPv6 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

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	Added ipv6 keyword.
	4.0(1)	This command was introduced.

Usage Guidelines	Use the track interface command to track the line protocol status or IPv4 or IPv6 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.

This command does not require a license.

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)#
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
show track	Displays information about object tracking.
track {ip ipv6} route reachability	Tracks the state of an IPv4 or IPv6 route reachability.
vrf member	Tracks an object in a nondefault VRF.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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** *interface-num* | **vlan** *vlan-num* | **port-channel** *channel-group-num* }
priority *value*

no track interface

Syntax Description

ethernet <i>interface-num</i>	The virtual router interface for which to track priority. The range is from 1 to 255.
vlan <i>vlan-num</i>	The VLAN for which to track priority.
port-channel <i>channel-group-num</i>	The port-channel group for which to track priority.
priority <i>value</i>	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.

Defaults

Disabled

Command Modes

VRRP configuration mode

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modified
4.0(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.

This command does not require a license.



Note

Interface state tracking will not be operational unless you enable preemption on the interface.

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to enable interface state tracking for a virtual router:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# track interface ethernet 2/2 priority 2
```

Related Commands

Command	Description
feature vrrp	Enables VRRP.
show vrrp	Displays VRRP configuration information.
track (VRRP)	Tracks an object to modify the VRRP priority.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>object-id</i>	Tracking ID. The range can be from 1 to 500.
	<i>ip-prefix/length</i>	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

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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.

This command does not require a license.

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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
track ipv6 route reachability	Tracks an IPv6 route reachability.
vrf member	Tracks an object in a nondefault VRF.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

track ipv6 route

To configure object tracking on an IPv6 route, use the **track ipv6 route** command. To remove the object tracking for this route, use the **no** form of this command.

track *object-id* **ipv6 route** *ipv6-prefix/length* **reachability**

no track *object-id* [**force**]

Syntax Description	<i>object-id</i>	Tracking ID. The range can be from 1 to 500.
	<i>ipv6-prefix/length</i>	Prefix of route to track. The IPv6 prefix format is A:B::C:D/length. The length can be from 1 to 128.
	reachability	Tracks the reachability state of an IPv6 route.
	force	(Optional) Completely removes the object tracking instance.

Command Default	None

Command Modes	Global configuration

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines

Use the **track ipv6 route** command to track the status of an IPv6 route. 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.

This command does not require a license.

Examples

This example shows how to track an IPv6 route:

```
switch(config)# track 1 ipv6 route 2001:0DB8::/8 reachability
switch(config-track)#
```

Related Commands	Command	Description
	show track	Displays information about object tracking.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
track ip route	Tracks an interface.
vrf member	Tracks an object in a nondefault VRF.

Send document comments to nexus7k-docfeedback@cisco.com

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		
<i>object-id</i>		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

SupportedUserRoles	network-admin vdc-admin

Command History	Release	Modification
	4.2(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:

Send document comments to nexus7k-docfeedback@cisco.com

- **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.

This command does not require a license.

Examples

This example shows how to create a track list of two objects and AND their state:

```
switch(config)# track 1 boolean and
switch(config-track)#object 33
switch(config-track)#object 30
```

This example shows how to configure a track list with an up threshold of 70% and a down threshold of 30%:

```
switch# config t
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
```

This example shows how to configure a track list with an up weight threshold of 30 and a down threshold of 10:

```
switch# config t
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
```

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.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>seconds</i> Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.				
Defaults	1 second				
Command Modes	Virtual interface configuration				
Supported User Roles	network-admin vdc-admin				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(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 Enterprise Services license.				
Examples	The following example sets the retransmit delay value to 3 seconds: <pre>switch(config)# router ospf 201 switch(config-router)# area 22 virtual-link 192.0.2.1 switch(config-router-vlink)# transmit-delay 3</pre>				

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

transmit-delay (OSPFv3 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	<i>seconds</i>	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Defaults	1 second

Command Modes	Virtual interface configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(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 Enterprise Services license.

Examples	This example sets the retransmit delay value to 3 seconds:

```
switch(config)# router ospfv3 201
switch(config-router)# area 22 virtual-link 192.0.2.1
switch(config-router-vlink)# transmit-delay 3
```

Send document comments to nexus7k-docfeedback@cisco.com



V Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter V.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

vrf

To create a VPN routing and forwarding instance (VRF) or enter the VRF configuration mode and configure submode commands for the Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS), 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

<i>name</i>	Name of the VRF.
management	Specifies a configurable VRF name.

Command Default

None

Command Modes

Address-family configuration
Router configuration
VRF configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Each VRF mode serves as a separate instance within the IS-IS process. All configuration commands available in the global configuration mode are available in the new VRF mode. For example, each VRF mode must have its own NET configured for that particular instance to be operational. All EXEC commands can be specified to be per-VRF; else, with no arguments, it will be applied to the default VRF. Note that interfaces belong to a particular VRF and the appropriate interface will only be applied to the particular interface with the `ip/ipv6 router isis` command.

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:

- **address-family**—Configures an address family. See the **address-family (BGP)** command for additional information.
- **authentication key-chain**—Sets the authentication key chain string. See the **authentication key-chain** command for additional information.
- **authentication-check**—Checks the authentication. See the **authentication-check** command for additional information.

Send document comments to nexus7k-docfeedback@cisco.com

- **authentication-type**— Sets the authentication type. See the **authentication-type** command for additional information.
- **default-information**— Controls the origination of a default route. See the **default-information originate (IS-IS)** command for additional information.
- **distance**— Configures the administrative distance. See the **distance (IS-IS)** command for additional information.
- **distribute**— Distributes routes between ISIS levels. See the **distribute** command for additional information.
- **exit**— Exits from the current command mode.
- **graceful-restart**— Enables the graceful restart for IS-IS process. See the **graceful-restart (BGP)** command for additional information.
- **hostname**— Configures the dynamic hostname for IS-IS. See the **hostname dynamic** command for additional information.
- **is-type**— Configures the IS type for this IS-IS process. See the **is-type** command for additional information.
- **log-adjacency-changes**— Logs the changes in adjacency state. See the **log-adjacency-changes (IS-IS)** command for additional information.
- **lsp-gen-interval**— Configures the LSP generation interval. See the **lsp-gen-interval** command for additional information.
- **lsp-mtu**— Sets the LSP MTU. See the **lsp-mtu** command for additional information.
- **max-lsp-lifetime**— Sets the maximum LSP lifetime. See the **max-lsp-lifetime** command for additional information.
- **maximum-paths**— Sets the maximum paths per destination. See the **maximum-paths (IS-IS)** command for additional information.
- **net**— Configures the Network Entity Title for this IS-IS process. See the **net** command for additional information.
- **no**— Negates a command or set its defaults.
- **redistribute**— Redistributes the information from another routing protocol. See the **redistribute (IS-IS)** command for additional information.
- **reference-bandwidth**— Changes the reference bandwidth used for setting interface metric. See the **reference-bandwidth** command for additional information.
- **set-overload-bit**— Signals other routers not to use us for transit. See the **set-overload-bit** command for additional information.
- **shutdown**— Shuts down this IS-IS process. See the **shutdown (IS-IS)** command for additional information.
- **spf-interval**— Configures the SPF interval. See the **spf-interval** command for additional information.
- **summary-address**— Configures the IP address summaries. See the **summary-address** command for additional information.
- **wide-metric-only**— Advertises only wide metric. See the **wide-metric-only** command for additional information.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following command shows how to enter VRF configuration mode:

```
switch(config)# router isis 100  
switch(config-router)# vrf management  
switch(config-router-vrf)#
```

Related Commands

Command	Description
address-family	Enters the address family mode or a VRF address-family mode.
feature isis	Enables IS-IS on the router.
router isis	Enables IS-IS.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

vrf context

To create a virtual routing and forwarding instance (VRF) and enter VRF configuration mode, use the **vrf** router BGP configuration command. To remove a VRF entry, use the **no** form of this command.

vrf context {*name* | **management**}

no vrf context {*name* | **management**}

Syntax Description

<i>name</i>	Name of the VRF. The <i>name</i> can be any case-sensitive, alphanumeric string up to 32 characters.
management	Specifies a configurable VRF name.

Command Default

This command has no default settings.

Command Modes

Neighbor address-family configuration
Router bgp configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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:

- **address-family**—Configures an address-family. See the **address-family (BGP)** command for additional 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. 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. This 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.

Send document comments to nexus7k-docfeedback@cisco.com



Note

All route reflectors must maintain stable sessions between all peers in the cluster. If stable sessions cannot be maintained, then overlay route reflector clusters should be used instead (route reflectors with different cluster IDs).

- **exit**—Exits from the current command mode.
- **graceful-restart**—Configure Graceful Restart functionality. See the **graceful-restart (BGP)** command for additional information.
- **graceful-restart-helper**—Configure Graceful Restart Helper mode functionality. See the **graceful-restart (BGP)** command for additional information.
- **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 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** and **show bgp ipv6 neighbors** commands.

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. See the **neighbor** command for additional information.
- **no**—Negates a command or set its defaults
- **router-id ip-addr**—Specifies the IP address to use as the router-id.
- **timers bestpath-timeout**—Configures the bestpath timeout in seconds. Range: 1 to 3600. Default: 300.

Examples

The following command shows how to enter VRF configuration mode:

```
switch(config)# router bgp 64496
switch(config-router)# vrf context management
switch(config-router-vrf)#
```

The following example shows how to set the local router as one of the route reflectors serving the cluster. You configure the cluster ID to identify the cluster.

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.168.70.24 route-reflector-client
switch(config-router)# cluster-id 10.0.1.2
```

Send document comments to nexus7k-docfeedback@cisco.com

vrf member

To configure object tracking on a virtual routing and forwarding (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	<i>vrf-name</i> VRF name. The name can be any case-sensitive alphanumeric string up to 64 characters.						
Command Default	None						
Command Modes	Global configuration						
Supported User Roles	network-admin vdc-admin						
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.		
Release	Modification						
4.0(1)	This command was introduced.						
Usage Guidelines	Use the vrf member command in object tracking configuration mode to track objects in a nondefault VRF. This command does not require a license.						
Examples	This example shows how to track an IP route in vrf Red: <pre>switch(config)# track 1 ip route 10.10.10.0/8 reachability switch(config-track)# vrf member Red</pre>						
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show track</td><td>Displays information about object tracking.</td></tr><tr><td>track ip route</td><td>Tracks an interface.</td></tr></table>	Command	Description	show track	Displays information about object tracking.	track ip route	Tracks an interface.
Command	Description						
show track	Displays information about object tracking.						
track ip route	Tracks an interface.						

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>number</i>
	The 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.

Defaults

None

Command Modes

VRRP configuration mode

Supported User Roles

network-admin
VDC administrator

Command History

Release	Modified
4.0(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.

This command does not require a license.

Examples

This example shows how to create a VRRP group:

```
switch(config-if-vrrp)# vrrp 7
```

This example shows how to create a VRRP group and configure an IPv4 address for the group:

```
switch# config terminal
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 7
switch(config-if-vrrp)# address 10.0.0.10
switch(config-if-vrrp)# no shutdown
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com



W Commands

This chapter describes the Cisco NX-OS unicast routing commands that begin with the letter W.

weighting

To specify the initial weighting value of the Gateway Load Balancing Protocol (GLBP) gateway, use the **weighting** command. To restore the default values, use the **no** form of this command.

weighting *maximum* [**lower** *lower*] [**upper** *upper*]

no weighting *maximum* [**lower** *lower*] [**upper** *upper*]

Syntax Description	<i>maximum</i>	Maximum weighting value. The range is from 1 to 254. The default value is 100.
	lower <i>lower</i>	(Optional) Specifies a lower weighting value. The range is from 1 to the specified maximum weighting value. The default value is 1.
	upper <i>upper</i>	(Optional) Specifies an upper weighting value. The range is from the lower weighting to the maximum weighting value. The default value is the specified maximum weighting value.

Defaults	The default gateway weighting value is 100 and the default lower weighting value is 1.

Command Modes	GLBP configuration

Supported User Roles	Network Administrator VDC Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

Usage Guidelines

The weighting value of a virtual gateway is a measure of the forwarding capacity of the gateway. If a tracked interface on the router fails, the weighting value of the router may fall from the maximum value to below the lower threshold, causing the gateway to give up its role as a virtual forwarder. When the weighting value of the gateway rises above the upper threshold, the gateway can resume its active virtual forwarder role.

Use the **glbp weighting track** and **track** commands to track an interface. If the interface goes down, GLBP reduces the weighting for the gateway by the specified value.

This command does not require a license.

Examples

This example shows how to set the weighting of the gateway for GLBP group 10:

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# weighting 110 lower 95 upper 105
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
track	Configures an interface to be tracked.

Send document comments to nexus7k-docfeedback@cisco.com

weighting track

To specify a tracking object where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the availability of the object being tracked, use the **weighting track** command. To remove the tracking, use the **no** form of this command.

weighting track *object-number* [**decrement** *value*]

no weighting track *object-number* [**decrement** *value*]

Syntax Description

<i>object-number</i>	Object number that represents an item to be tracked. Use the track command to configure the tracked object. The range is from 1 to 500.
decrement <i>value</i>	(Optional) Specifies an amount by which the GLBP weighting for the router is decremented (or incremented) when the interface goes down (or comes back up). The range is from 1 to 255. The default is 10.

Defaults

The default decrement value is 10.

Command Modes

GLBP configuration

Supported User Roles

Network Administrator
VDC Administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **weighting track** command ties the weighting of the GLBP gateway to the availability of its interfaces. This command is useful for tracking interfaces that are not configured for GLBP; for instance, you can track the interface that connects the gateway to the IP network.

When a tracked interface goes down, the GLBP gateway weighting decreases by the configured decrement value. For each GLBP group, you can track a separate list of interfaces.

When the tracked interface comes back up, GLBP increments the weighting by the same amount.

When multiple tracked interfaces are down, the configured weighting decrements are cumulative.

Use the **track** command to configure each interface that you want to track.

This command does not require a license.

Examples

This example shows that ethernet interface 1/1 tracks two interfaces represented by the numbers 1 and 2. If interface 1 goes down, the GLBP gateway weighting decreases by the default value of 10. If interface 2 goes down, the GLBP gateway weighting decreases by 5.

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# interface fastethernet 0/0
switch(config-if)# glbp 10
switch(config-glbp)# weighting track 1
switch(config-glbp)# weighting track 2 decrement 5
```

Related Commands

Command	Description
glbp	Enters GLBP configuration mode and creates a GLBP group.
weighting	Specifies the initial weighting value of a GLBP gateway.
track	Configures an interface to be tracked.

Send document comments to nexus7k-docfeedback@cisco.com

wide-metric-only

To advertise wide metric links only, use the **wide-metric-only** configuration mode command. To remove the restriction, use the **no** form of this command.

wide-metric-only

no wide-metric-only

Syntax Description	This command has no arguments or keywords.

Command Default	None

Command Modes	Router configuration VRF configuration

Supported User Roles	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Metric values are assigned to a link and are used to calculate the path cost from the links to the destination points. The metric styles are as follows:

- Wide metrics—Metric value ranges from 1 to 16777214.
- Narrow metrics—Metric value ranges from 1 to 63.

The **wide-metric-only** command advertises only the links that are assigned a wide metric value.

Examples	The following command shows how to advertise only wide metric links:

```
switch(config)# router isis 100  
switch(config-router)# vrf management  
switch(config-router-vrf)# wide-metric-only
```

The following command shows how to remove the wide-metric link only restriction:

```
switch(config)# router isis 100  
switch(config-router)# vrf management  
switch(config-router-vrf)# no wide-metric-only
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
exit	Exits the current configuration mode.
feature isis	Enables IS-IS on the router.
no	Negates a command or sets its defaults.
router isis	Enables IS-IS.
vrf	Creates a VPN routing and forwarding instance (VRF) or enters the VRF configuration mode.